EUROSMART
The Voice of the Digital Security Industry

NIS2 - Simplification without Compromising Cybersecurity

Eurosmart Recommendations on the Proposal Amending Directive (EU) 2022/2555 (NIS2)

Eurosmart welcomes the Commission's proposal to simplify and improve the implementation of Directive (EU) 2022/2555 (NIS2) in line with the CSA 2 proposal and supports the objective of reducing unnecessary regulatory burden while maintaining a high level of cybersecurity across the Union.

The proposal contains several positive elements, including the introduction of post-quantum cryptography in national cybersecurity strategies, the recognition of cyber posture certification schemes, and the adaptation of scope criteria for certain categories of entities.

At the same time, several provisions would benefit from clarification or adjustment in order to preserve legal certainty, avoid unintended consequences and ensure that simplification efforts do not weaken cybersecurity or create inconsistencies with other Union legislation.

Eurosmart therefore proposes targeted amendments in six key areas:

- Digital Identity and Trust Services;
- Cybersecurity Certification;
- Post-Quantum Cryptography;
- Supply Chain Security;
- Scope and Harmonisation of NIS2;
- Governance, Reporting and ENISA Registry.

1. Digital Identity and Trust Services

1.1 Recognising Critical Actors in the European Digital Identity Ecosystem

Eurosmart strongly welcomes the inclusion of European Digital Identity Wallets providers (EUDIW) and European Business Wallets (EBW) within the scope of NIS2 as Essential Entities (**Proposal #1**). These actors will constitute critical components of the Union's digital identity infrastructure and will play a central role in supporting secure digitalisation across Europe.

1.2 Clarifying the Interplay between NIS2 and eIDAS

However, the inclusion of these entities also creates new interactions between NIS2 and Regulation (EU) No 910/2014 (eIDAS). Particular attention should be given to the relationship between both frameworks regarding security breach management, incident reporting, certification obligations and supervisory arrangements. Clarification is necessary to avoid duplication of requirements and ensure legal certainty for regulated entities (**Proposal #1**).

1.3 Completing the Scope of Essential Digital Identity Infrastructure

Eurosmart further considers that additional actors supporting the European Digital Identity ecosystem should be recognised as Essential Entities. Personal Identification Data (PID) Providers perform critical functions relating to identity verification, authentication and trust services and should be explicitly classified as Essential Entities (**Proposals #2 and #13**).

Likewise, entities responsible for the issuance of Digital Travel Credentials process highly sensitive identity data and support border management actions. Given the criticality, they should also be explicitly classified as Essential Entities (**Proposals #3 and #12**).

1.4 Avoiding Duplication through Recognition of Equivalent Requirements

Finally, where entities are already subject to equivalent obligations under eIDAS, a mechanism should be established to recognise those obligations for the purposes of NIS2 compliance. Such an approach would reduce administrative burden, avoid duplication and provide greater legal certainty for both regulated entities and supervisory authorities (**Proposal #26**).

2 Cybersecurity Certification

Eurosmart welcomes the introduction of European cybersecurity certification schemes on the cyber posture of entities as a mechanism for demonstrating compliance with Article 21 of NIS2 - cybersecurity risk-management measures (**Proposal #4**).

Such schemes would provide a harmonised and practical framework for assessing cybersecurity maturity across sectors.

2.1 Ensuring Stakeholder Involvement in Certification Schemes

The preparation of the cyber-posture schemes should therefore involve all relevant stakeholders, including the NIS Cooperation Group, competent supervisory authorities, industry representatives and the entities that will ultimately be subject to certification (**Proposal #29**).

2.2 Preserving Subsidiarity Principles and Existing National Certification Frameworks

Eurosmart also considers it essential to clarify that implementing acts adopted pursuant to Article 21(5) and specifying how cybersecurity risk-management measures must be implemented, should not affect the ability of Member States to require the use of ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes, nor prevent Member States from maintaining or introducing national cybersecurity certification or accreditation requirements where permitted under Union law (**Proposal #19**).

Finally, cyber-posture certification schemes should support the objectives of harmonisation and simplification while preserving the flexibility necessary to address specific national cybersecurity needs and existing certification frameworks. Such schemes should complement, rather than inadvertently restrict, the cybersecurity measures available to Member States and regulated entities.

3 Post-Quantum Cryptography (PQC)

3.1 Recognising the Quantum Computing Threat

Eurosmart strongly supports the explicit recognition of cybersecurity risks stemming from quantum computing and welcomes the inclusion of post-quantum cryptography within national cybersecurity strategies (**Proposal #5**).

The transition to PQC will constitute one of the most significant cybersecurity challenges of the coming decade. The proposal correctly identifies the need to address the impact of quantum computing on cybersecurity, however, further guidance should be provided to support Member States in the definition and implementation of their migration strategies.

3.2 Establishing Comprehensive PQC Migration Strategies

To support effective implementation, national strategies should include comprehensive inventories of cryptographic assets, identification and classification of use cases according to their criticality, migration plans with clear milestones, and risk mitigation measures where migration cannot be completed within the expected timelines (**Proposal #17**).

3.3 Defining Clear Timelines for the Transition to PQC

Eurosmart supports the establishment of migration targets for critical use cases by 2030 and for remaining use cases by 2035, together with appropriate monitoring mechanisms (**Proposal #18**).

By providing greater clarity on migration planning, timelines and risk management, national cybersecurity strategies would become a key instrument for preparing Europe's digital infrastructure for the PQC challenge.

4 Supply Chain Security

Eurosmart welcomes the Commission's intention to develop guidelines regarding information requests used by essential and important entities to assess supply chain security (**Proposal #6**).

Given the practical experience of industry stakeholders, Eurosmart believes that industry should be closely involved in the preparation of these guidelines, including through dedicated expert groups where appropriate Such involvement would help ensure that the resulting guidance is practical, proportionate and aligned with operational realities.

5 Scope and Harmonisation of NIS2

5.1 Adapting NIS2 Scope Requirements for Small Mid-Cap Enterprises

Eurosmart supports the proposal to extend the size-cap threshold from medium-sized enterprises to small mid-cap enterprises (**Proposal #14**). This pragmatic adjustment contributes to the broader objective of reducing compliance burdens while maintaining an appropriate level of cybersecurity.

5.2 Maintaining Domain Name System (DNS) Service Providers within the Scope of NIS2

At the same time, Eurosmart believes that Domain Name System (DNS) service providers should remain within the scope of NIS2 (**Proposal #11**). As recognised in Directive (EU) 2022/2555 itself, DNS service providers are key to maintaining the integrity, availability and stability of the internet and continue to play a critical role in supporting the digital economy and society.

5.3 Clarifying the Scope of Managed Service Providers

Further clarification is necessary regarding the definition and scope of managed service providers **(Proposals #9 and #16).** The current wording creates uncertainty as to which entities are covered by managed service providers; whether managed services are limited to business-to-business relationships and regarding the treatment of entities whose activities may simultaneously fall within the definition of managed services and another category of entities covered by NIS2.

A number of entities already covered by the Directive, may also provide managed services as part of their primary activity, entailing that they fall within two types of entities for the same activity.

On this point, the Commission should develop guidance clarifying the scope of managed services and the treatment of entities carrying out both managed services and activities falling within other NIS2 categories.

5.4 Preserving National Possibility to Ensure a Higher Level of Cybersecurity

Finally, Eurosmart believes that NIS2 should preserve its minimum-harmonisation character (**Proposals #8 and #15**). In line with subsidiarity principles, the proposal should not prevent Member States from adopting or maintaining more stringent cybersecurity requirements where justified by national circumstances. Such a possibility remains particularly important where cybersecurity requirements contribute to the protection of national interests. Hence, cybersecurity requirements applicable to essential and important entities may be closely linked to national security considerations, which remain the sole responsibility of each Member State

In addition, future Commission implementing acts specifying the technical, methodological and sectoral requirements applicable to the cybersecurity risk-management measures under Article 21 should not affect the ability of Member States to require the use of ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes (**Proposal #20**).

5.5 Ensuring Consistency with the Union Cloud Sovereignty Framework under the Cloud and AI Development Act (CADA).

Ensuring coherence between NIS2 and the Union Cloud Sovereignty Framework established under the Cloud and AI Development Act (CADA) will be essential to strengthening the resilience and security of critical sectors across the Union **(Proposals #10 and #18).**

Entities operating in sectors of high criticality increasingly rely on cloud computing services to support essential functions. Sovereignty-related risks, including strategic dependencies, foreign control, unlawful access to data and continuity-of-service risks, are becoming increasingly relevant components of cybersecurity and operational resilience. In this context, the Union Cloud Sovereignty Framework can serve as an important tool for supporting risk-management and cloud sourcing decisions.

Eurosmart strongly advocates for an approch under the CADA proposal **whereby entities covered by NIS2 assess sovereignty-related risks associated with cloud sourcing decisions and rely on cloud computing services recognised at Union Assurance Level 3 or Union Assurance Level 4 for services supporting essential functions.**

The Commission should ensure that policy measures, guidance and implementation activities developed under NIS2 and CADA remain fully aligned. A coherent approach between both frameworks would reduce fragmentation, facilitate compliance and strengthen the resilience, security, digital sovereignty and strategic autonomy of critical sectors across the Union.

6 Governance, Incident Reporting and ENISA Registry

6.1 Strengthening the Role of the NIS Cooperation Group

Eurosmart proposes stronger consultation mechanisms within the implementation process of NIS2. In particular, the NIS Cooperation Group should be systematically consulted when the Commission prepares assessments under Article 21(5), ensuring that Member State expertise is fully considered (**Proposal #21**).

6.2 Improving Legal Certainty and Consistency of Incident Reporting Requirements

Regarding incident reporting, Eurosmart believes that, for legal clarity, ransomware-related reporting requirements should be included directly in Article 23 rather than delegated to future implementing acts (**Proposals #23**).

Eurosmart also supports aligning incident notification timelines with broader Union legislation (**Proposal #25**). Significant cybersecurity incidents and personal data breaches frequently arise from the same event and often trigger parallel reporting obligations. Aligning the NIS2 reporting deadline with the proposed 96-hour GDPR deadline would reduce administrative burden, improve consistency across the Union legal framework and facilitate the submission of higher-quality notifications.

6.3 Aligning Reporting Obligations for Trust Service Providers

Furthermore, the specific 24-hour reporting obligation applicable only to trust service providers should be removed (**Proposal #26**). A differentiated reporting deadline is not justified and creates disproportionate compliance burdens compared to those applicable to other essential and important entities. Trust service providers should therefore be subject to the same reporting timelines as other entities covered by Directive (EU) 2022/2555.

6.4 Avoiding the Unnecessary Centralisation of Sensitive Information

Finally, Eurosmart considers that the proposed ENISA registry should be more targeted and proportionate (**Proposals #7, #29 and #30**). National authorities already maintain registries of essential and important entities under NIS2. Any Union-level registry should be limited to information strictly necessary to support ENISA's tasks and facilitate cross-border cooperation. Competent authorities should have access to the information contained in the registry where necessary for the exercise of their responsibilities under the Directive. At the same time, Member States should retain the possibility not to transmit information where such transmission would adversely affect their essential security interests.

Conclusion

Eurosmart supports the objectives of the proposal and welcomes efforts to simplify the implementation of NIS2. The targeted amendments proposed in this paper would improve legal certainty, preserve flexibility for Member States, avoid duplication with other Union legislation and ensure that simplification measures continue to support a high level of cybersecurity throughout the Union.

Summary of Recommendations

Eurosmart welcomes the objective of simplifying and improving the implementation of Directive (EU) 2022/2555 while preserving a high level of cybersecurity across the Union.

Eurosmart recommends:

Digital Identity and Trust Services

- **Proposal #1** - Clarify the interplay between NIS2 and Regulation (EU) No 910/2014 (eIDAS) for European Digital Identity Wallets (EUDIW) and European Business Wallets (EBW).
- **Proposals #2 and #13** - Classify Personal Identification Data (PID) Providers as Essential Entities.
- **Proposals #3 and #12** - Classify entities responsible for the issuance of Digital Travel Credentials as Essential Entities.
- **Proposal #26** - Introduce a mechanism recognising equivalent obligations under eIDAS and establishing a presumption of conformity with NIS2 requirements.

Cybersecurity Certification

- **Proposals #4 and #29** - Ensure the preparation of European cyber-posture certification schemes involves relevant stakeholders, including industry, supervisory authorities and the NIS Cooperation Group.
- **Proposal #28** - Correct the legal reference to Article 74 of the CSA2 proposal.
- **Proposal #19** - Clarify that implementing acts adopted under Article 21(5) do not affect Member States' ability to require European or national cybersecurity certification schemes where permitted under Union law.

Post-Quantum Cryptography

- **Proposals #5 and #17** - Strengthen provisions on migration to post-quantum cryptography through inventories, migration plans, timelines and risk mitigation measures.

Supply Chain Security

- **Proposal #6** - Ensure industry participation in the preparation of supply-chain security questionnaires and publish the related guidelines without undue delay.

ENISA Registry

- **Proposals #7, #29 and #30** - Limit the scope of the ENISA registry to what is strictly necessary, provide access for competent authorities, and preserve Member States' ability to withhold information where national security interests are concerned.

Scope of NIS2

- **Proposal #11** - Maintain DNS service providers within the scope of NIS2.
- **Proposal #14** - Support the extension of the size-cap threshold to small mid-cap enterprises.
- **Proposals #9 and #16** - Clarify the scope and definition of managed service providers, including the treatment of ICT services and services provided beyond business-to-business relationships.
- **Proposals #10 and #18** - Recognise and mitigate cybersecurity risks associated with cloud dependencies and third-country exposure.

Cybersecurity Requirements and Harmonisation

- **Proposals #8, #15 and #20** - Preserve the minimum-harmonisation approach of NIS2 and maintain Member States' ability to adopt higher cybersecurity requirements where necessary.

Governance and Consultation

- **Proposal #21** - Ensure systematic consultation of the NIS Cooperation Group when preparing assessments under Article 21(5).

Incident Reporting

- **Proposals #22 and #23** - Include ransomware-related reporting requirements directly in Article 23 rather than through future implementing acts.
- **Proposal #25** - Align the NIS2 incident-notification deadline with the proposed GDPR deadline of 96 hours.
- **Proposal #26** - Remove the specific 24-hour reporting deadline applicable to trust service providers and align them with the general reporting framework.

#	Article	Original Text	Amendment	Rationale
1.	Recital 5	The proposal introduces providers of European Digital Identity Wallets (EUDIW) and European Business Wallets (EBW) as essential entities.	Support the inclusion of EUDIW providers and EBW providers as essential entities. **Amend Recital 5 as follows:** In order to ensure legal certainty and avoid overlaps or inconsistencies, the interplay between this Directive and Regulation (EU) No 910/2014 should be clearly specified. In particular, where obligations concerning security breaches, incident reporting, certification or supervision overlap, duplication of requirements should be avoided. The Commission should, where appropriate, adopt implementing acts or issue guidelines specifying such interplay.	Eurosmart welcomes the inclusion of EUDIW and EBW providers as essential entities, reflecting their critical role in the Union's digital identity ecosystem. However, the proposal creates potential overlaps between NIS2 and Regulation (EU) No 910/2014 (eIDAS), particularly regarding security breach management, incident reporting, certification and supervision. Clarification is required to ensure legal certainty and avoid duplicate obligations.
2.	New recital 5a	The proposal introduces providers of European Digital Identity Wallets (EUDIW) and European Business Wallets (EBW) as Essential Entities but does not address Personal Identification Data (PID) Providers established under Regulation (EU) No 910/2014.	**New recital 5a:** Providers of Personal Identification Data (PID) established pursuant to Regulation (EU) No 910/2014 are a key component of the European Digital Identity ecosystem and contribute to secure identification, authentication and the exchange of electronic documents, including electronic attestations of attributes. Given their critical role in the functioning, security and trustworthiness of the European Digital Identity framework, they should be classified as Essential Entities under this Directive.	PID Providers are a core component of the European Digital Identity ecosystem and support critical functions related to identity verification, authentication and trust services. Their compromise could significantly affect the security and reliability of the Union's digital identity infrastructure.
3.	New recital 5b	The proposal does not address entities	**New recital 5b**	Digital Travel Credential issuers process highly sensitive personal data, including identity

#	Article	Original Text	Amendment	Rationale
		responsible for the creation and issuance of Digital Travel Credentials under COM(2024) 670 final and COM(2024) 671 final.	Entities responsible for the creation and issuance of Digital Travel Credentials pursuant to [Proposal on the EU Digital Travel application] and [Proposal on the issuance of and technical standards for Digital Travel Credentials based on identity cards] play a critical role in the protection of travellers' identity data and in facilitating secure border crossings. Given their importance for the security and trustworthiness of the Union's digital travel ecosystem, they should be classified as Essential Entities under this Directive.	information and facial images, and support border management functions. Their compromise could have significant consequences for both cybersecurity and trust in digital travel infrastructures.
4.	Recital 7	The proposal introduces the possibility for essential and important entities to rely on a certificate on the cyber posture under a European cybersecurity certification scheme to demonstrate compliance with Article 21 of Directive (EU) 2022/2555.	**Amend Recital 7 as follows:** The development of such a scheme will benefit from the adoption of implementing acts on the technical, methodological and sectoral requirements concerning cybersecurity risk-management measures under Directive (EU) 2022/2555. **The preparation of European cybersecurity certification schemes on the cyber posture of entities should involve relevant stakeholders, including the NIS Cooperation Group, competent supervisory authorities, industry, and essential and important entities**.	Eurosmart welcomes the introduction of cyber posture certification schemes as a harmonised mechanism enabling essential and important entities to demonstrate compliance with Article 21. Given the potential impact of such schemes on both supervision and compliance activities, their preparation should benefit from the expertise of all relevant stakeholders.
5.	Recital 8	The proposal requires Member States to adopt policies for the transition to post-quantum cryptography (PQC) as part	**Amend Recital 8 as follows:** […] Member States should be required to adopt policies for the migration to post-quantum cryptography (PQC) as part of their national cybersecurity strategy. **Those policies should include,**	Eurosmart welcomes the explicit recognition of cybersecurity risks stemming from quantum computing and the inclusion of post-quantum cryptography in national cybersecurity strategies. However, additional guidance is required to support the effective and consistent

#	Article	Original Text	Amendment	Rationale
		of their national cybersecurity strategies.	**in particular, the identification and inventory of use cases based on their criticality, a comprehensive inventory of cryptographic assets, the establishment of migration plans with clear timelines, including for critical use cases by 2030 and for other use cases by 2035, as well as risk assessment and mitigation measures where migration cannot be achieved in due time**. […]	implementation of migration policies across Member States.
6.	Recital 9	The proposal provides for the development of guidelines recommending an appropriate level of detail, structure and format for information requests used by important and essential entities to assess supply-chain security.	**Add the following sentence at the end of Recital 9:** The Commission should ensure the close involvement of relevant industry stakeholders in the preparation of those guidelines, including, where appropriate, through an ad hoc expert group. Those guidelines should be published without undue delay.	Eurosmart welcomes the development of such guidelines, which will help reduce the burden on suppliers responding to cybersecurity-related information requests from important and essential entities. Given the practical experience of industry stakeholders, they should be closely associated with the preparation of the guidelines. Early publication is also important to provide timely support to European industry and promote harmonised implementation across the Union.
7.	Recital 12	The proposal establishes a registry of essential and important entities to be maintained by ENISA.	**Amend Recital 12 as follows:** Given the cross-border dimension of certain essential and important entities and the need to facilitate cooperation between competent authorities, ENISA should maintain a registry of entities for which information is necessary to support the tasks entrusted to it under this Directive. In accordance with the principles of necessity and proportionality, that registry should be limited to entities involved in	National authorities already maintain registries of essential and important entities pursuant to Article 3(3) and (4) of Directive (EU) 2022/2555. The establishment of an ENISA registry should therefore be limited to what is necessary to support ENISA's tasks and cross-border cooperation. Limiting the scope of the registry would reduce cybersecurity risks associated with the centralisation of sensitive information and

#	Article	Original Text	Amendment	Rationale
			cross-border activities and should contain only the information strictly necessary for the performance of those tasks. Competent authorities should have access to the information contained in the registry where necessary for the exercise of their responsibilities under this Directive. Taking due account of cybersecurity risks associated with the centralisation of sensitive information and of the responsibility of Member States for national security, Member States should retain the possibility not to transmit information to the registry where they consider that such transmission would adversely affect their essential national security interests.	avoid unnecessary duplication of information already held at national level.
8.	Recital 13	The proposal introduces a maximum harmonisation approach with regard to cybersecurity risk-management measures covered by implementing acts adopted under Article 21(5).	**Amend Recital 13 as follows:** At the same time, this Directive should not prevent Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, in accordance with Union law, in particular where such provisions are necessary to address specific national cybersecurity risks or safeguard national security, which remains the sole responsibility of each Member State pursuant to Article 4(2) TEU.	Directive (EU) 2022/2555 is based on a minimum harmonisation approach and should continue to allow Member States to adopt higher cybersecurity requirements where justified. Preserving such flexibility is particularly important where cybersecurity measures contribute to the protection of national security interests.
9.	Recital XX (new) and	Annex I refers to "ICT service management (Business-to-business)", while the definition of managed service provider in Article 6(39) does not	**Insert a new recital XX** Managed service providers contribute to the operation, management and security of network and information systems in a wide range of sectors and	The types of entities falling into the category "managed service provider" are unclear. 1. The definition of "managed service provider" in article 6(39) does not refer to any business-to-

#	Article	Original Text	Amendment	Rationale
	Annex I, point 9 of Directive (EU) 2022/2555	contain any business-to-business limitation.	use cases. Such services may be provided to businesses, public entities or individuals. In assessing whether an entity qualifies as a managed service provider under this Directive, due consideration should be given to the nature and significance of the managed services provided, irrespective of the category of customer to which those services are supplied. The European Commission should issue guidance to clearly support stakeholders in identifying which entities fall within that category. Moreover, certain entities may provide managed services as part of their activities falling within other categories of entities. In order to ensure a consistent application of this Directive across the Union, the European Commission should issue guidance on the treatment of such entities, including the determination of the applicable category of entity, supervisory arrangements, where managed services are provided alongside other regulated activities. **Amendment to Annex I, point 9** Replace: "ICT service management (Business-to-business)" with: *"ICT service management".*	business context. Yet, in Annex I, managed service providers are classified as "ICT service management (Business-to-business)" (item 9) which alludes that only managed service providers in the context of a business-to-business relationship are covered by NISD2, which is not the case as per the definition provided in article 6(39). It shall be noted that managed service providers acting in a non-business-to-business context may also have very substantial impacts on "[…] sectors and services of vital importance to key societal and economic activities in the internal market." (recital 6) and therefore shall not be excluded from the scope of the "managed service providers", e.g.: - managed service provider managing remotely the connected car of an individual - managed service provider managing individual internet box Therefore, it should be clarified in Annex I item 9, but also in a new recital that "managed service provider" are not limited to those acting in a business-to-business context. The scope of the category "managed service provider" is unclear. The definition provided in article 6(39) is extremely large and vague. Further guidance and clarification should be provided in a new recital to clearly support stakeholders in identifying which entities fall within that category.

#	Article	Original Text	Amendment	Rationale
				2. Some types of entities may carry out “services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely” (definition of managed service) as part of their activities, e.g.: - trust service provider managing a remote QSCD, remotely reinitializing a QSCD or remotely verifying the identity of an individual; - data centre service provider remotely managing its data centre In such case, it is unclear how these “services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely” should be treated under NISD2 by the entity. It should be clarified if that entity: - shall also declare itself as “managed service provider” for the scope covering these activities, on top of its other declaration for its other activities, - or shall not declare itself as “managed service provider”. Guidance is therefore needed here, since depending on the approach the rules for

#	Article	Original Text	Amendment	Rationale
				defining the type of entity (important or essential) as well as the jurisdiction are different.
10.	Recital XXa (new)	No provision addressing cybersecurity risks arising from dependencies on non-EU technologies, cloud service providers or exposure to third-country laws affecting critical digital services.	**Insert a new Recital XXa:** The increasing reliance of essential and important entities on cloud computing and remote data processes services create cybersecurity risks linked to excessive dependencies on individual service providers, non-Union technologies, loss of operational control, concentration of critical services, or exposure to third-country laws and regulatory requirements that may affect the confidentiality, integrity, availability or accessibility of data and services. As part of their cybersecurity risk-management measures, essential and important entities should assess such risks and adopt measures to ensure an adequate level of resilience, control, continuity and recoverability of critical digital services. The Commission should issue guidance on the identification and mitigation of such risks, taking into account relevant Union policies relating to cybersecurity, cloud security assurance and certification, strategic dependencies, technological sovereignty and trusted cloud services.	Essential and important entities increasingly rely on cloud computing and remote data processes to support critical functions that can also create cybersecurity risks arising from excessive dependencies on individual providers, concentration of critical services, reliance on non-EU technologies, or exposure to third-country laws with extraterritorial effects. These risks may affect the confidentiality, integrity, availability and accessibility of critical systems and data. NIS2 should therefore explicitly recognise such risks as part of cybersecurity risk-management measures and request entities to assess and mitigate them. The Commission should also provide guidance to ensure a consistent approach across the Union and maintain coherence with ongoing legislative development such as the Cloud and AI Act proposal and the future Cybersecurity certifiifaction scheme “EUCS”.
11.	Article 1(2) amending Article 2(2)(a)(iii) of	The proposal removes Domain Name System (DNS) service providers	**Article 2(2)(a)(iii):** Maintain the reference to “Domain Name System service providers”. **Article 3(1)(b):** Maintain DNS service providers within the categories of entities covered by the	Through these amendments, domain name system service providers (DNS service providers) are excluded from the scope of the directive.

#	Article	Original Text	Amendment	Rationale
	Directive (EU) 2022/2555 and Article 1(2) amending Article 3(1)(b)) of Directive (EU) 2022/2555	from the scope of Directive (EU) 2022/2555.	Directive.Delete the proposed amendments removing DNS service providers from the scope of Directive (EU) 2022/2555.	Yet, as indicated in recital (32) of NISD2, DNS service providers "[…] are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend.". Therefore, DNS service providers shall be kept in the scope of this directive. In addition these changes are not in line with the recital (2) which reads the following : "[…] Further, to support the Commission 's goal of cutting administrative costs by 25 % overall and by 35 % for small and medium-sized enterprises, the general size-cap rule set out in Directive (EU) 2022/2555, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC5, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of Directive (EU) 2022/2555, should be applied to Domain Name System service providers."
12.	Article 1(1) amending Article 2(2)(a) (new point (vi)); and Annex I	The proposal does not explicitly include entities responsible for the creation and issuance of Digital Travel Credentials among the categories of Essential Entities.	**Add a new point (vi) to Article 2(2)(a)** Entities responsible for the creation and issuance of Digital Travel Credentials pursuant to [COM(2024) 670 final] and [COM(2024) 671 final]. **Include such entities among the categories of Essential Entities listed in Annex I.**	Entities in charge of the creation and issuance of Digital Travel Credentials established by COM(2024) 670 final [Proposal on EU Digital Travel application] and COM(2024) 671 final [Proposal on the issuance of and technical standards for digital travel credentials based on identity cards] shall be classified as Essential Entities in the light of their criticity as to

#	Article	Original Text	Amendment	Rationale
	of Directive (EU) 2022/2555			- protection of sensitive data (legal identity and portrait of travelers) and - border crossing. As per the current status of these files, such entities may not necessarily fall in any existing categories defined in NISD2. In particular, such entities may not fall in the category “Non-qualified trust service providers” or “Qualified trust service providers”, as - it is unclear whether they will be required to issue Digital Travel Credential under the shape of Qualified Electronic Attestation of Attributes (QEAA), and - in some settings Digital Travel Credentials could be issued without any signing operation (e.g. creation), likely not to qualify as “Non-qualified trust service providers”. Therefore, Entities in charge of the creation and issuance of Digital Travel Credentials established by COM(2024) 670 final [Proposal on EU Digital Travel application] and COM(2024) 671 final [Proposal on the issuance of and technical standards for digital travel credentials based on identity cards] shall explicitly be included in the list of Essential Entities alongside “providers of European Digital Identity Wallets” and “providers of European Business Wallets”.

#	Article	Original Text	Amendment	Rationale
13.	Article 1(1) amending Article 2(2)(a) (new point (vii)); and Annex I of Directive (EU) 2022/2555	PID Providers are not explicitly included among the categories of Essential Entities. Depending on their qualification status and size, they may be classified as either Essential or Important Entities.	**Add a new point (vii) to Article 2(2)(a)** (vi) providers of Personal Identification Data (PID) pursuant to Regulation (EU) No 910/2014. **Include PID Providers among the categories of Essential Entities listed in Annex I.**	PID Providers (as established in the amended Regulation (EU) No 910/2014 of the European Parliament and of the Council) should also be introduced as essential entities as they are also instrumental for and part of the Union's digital infrastructure enabling secure identification and authentication and the exchange of electronic documents, including electronic attestations of attributes. As PID providers will issue signed credentials (PID), they will fall either in the category "Non-qualified trust service providers" or "Qualified trust service providers", depending on whether it decides to have its service qualified or not. Yet, where the PID provider falls in the category "Non-qualified trust service providers" and is an entity other than a large entity, it will be classified as important entity, unlike essential entity in the other cases. In the light of the importance and criticity of PID Providers, they shall always be classified as Essential Entity. Therefore, PID Providers shall explicitly be included in the list of Essential Entities alongside "providers of European Digital Identity Wallets" and "providers of European Business Wallets".
14.	Artile 1(2) amending	The proposal changes the size threshold from entities exceeding the ceilings for medium-sized enterprises		This amendment moves the threshold from entities which exceed the ceilings for medium-

#	Article	Original Text	Amendment	Rationale
	Article 3(a) and Recital 2 of Directive (EU) 2022/2555	to entities exceeding the ceilings for small mid-cap enterprises.		sized enterprises to entities which exceed the ceilings for small mid-cap enterprises. Eurosmart very much welcome this pragmatic approach
15.	Article 1(3) amending Article 5 of Directive (EU) 2022/2555	The proposal would prevent Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity where an implementing act has been adopted pursuant to Article 21(5).	**Delete the proposed amendment to Article 5.**	These modifications substantially change the initial approach whereby MS have the freedom of "[…] adopting or maintaining provisions ensuring a higher level of cybersecurity" if they want or deem necessary as enshrined in the current article 5. These modifications would deprive MS to do so and thus MS would be strictly limited to the cybersecurity provisions laid down in the implementing act(s) adopted in accordance with article 21.5 (if adopted). As such implementing act will have to be supported by a majority of Member States, its content will necessarily be the outcome of a compromise between various parties. **Therefore, this will very likely result in levelling down the overall cybersecurity of important and essential entities throughout EU**. Also the implementing act(s) "[…] laying down the

#	Article	Original Text	Amendment	Rationale
				technical and the methodological requirements, as well as sectoral requirements […]" could be adopted for any type of entities. In addition, **cybersecurity of important and essential entities is also likely to be directly relevant for national security of MS, which is not a EU competency but a national competency. Therefore, that amendment to NISD2 shall not deprive MS from adopting or maintaining provisions ensuring a higher level of cybersecurity**. This new approach also raises substantial issues: - The interplay between the proposed fifth subparagraph of Article 21(5), which would prohibit Member States from adopting or maintaining additional technical, methodological or sectoral cybersecurity requirements where an implementing act has been adopted, and Article 24(1) of Directive (EU) 2022/2555, which expressly allows Member States to require essential and important entities to use ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, is unclear. - **In particular, the proposed amendment creates legal uncertainty as to whether Member States would remain entitled**

#	Article	Original Text	Amendment	Rationale
				to require the mandatory use of ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes where an implementing act has been adopted pursuant to Article 21(5). This point should be clarified. Where an implementing act is adopted as per the amendment to article 21.5 (fifth paragraph), would it mean that MS **would not be allowed to require the use of national cybersecurity certification or cybersecurity accreditation such as SecNumCloud (France - cloud), C5 (Germany - cloud), CSPN/BSZ/LINCE (France/Germany/Spain - software) or qualification de sécurité (France)?** This should be clarified.
16.	Article 1(4)a (New) amending Article 6(39) of Directive (EU) 2022/2555	The definition of managed service provider refers to ICT products, networks, infrastructure, applications and network and information systems, but does not explicitly refer to ICT services.	**Amend Article 6(39) as follows:** means an entity that provides services related to the installation, management, operation or maintenance of ICT products, ICT services, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.	The definition provided in article 6(39) should also consider "ICT services", alongside "ICT products".

#	Article	Original Text	Amendment	Rationale
17.	Article 1(5) amending Article 7(2)(k) (proposed point k) of Directive (EU) 2022/2555	The proposal introduces a requirement for national cybersecurity strategies to address the transition to post-quantum cryptography.	**Amend Article 7(2)(k) as follows:** (k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies, **including the identification and inventory of use cases based on their criticality, and cryptographic assets, the establishment and monitoring of migration plans with clear timelines, including for critical use cases by 2030 and for other use cases by 2035, and the implementation of risk assessment and mitigation measures where migration cannot be achieved in due time.**	Eurosmart very much welcome this amendment which explicitly highlights the need to consider cybersecurity risks stemming from quantum computer and thus that each national cybersecurity strategy shall address the challenge of the transition to post quantum cryptography. However, the relevant aspects of that national cybersecurity strategy should be better detailed to support the definition and implementation by MS. As such the following aspects should be included: - Identification and inventory of critical use cases whose migration shall be achieved by 2030; - Identification and inventory of medium and low-level use case whose migration shall be achieved by 2035; - Comprehensive inventory of cryptographic algorithms used for each of these use cases; - Definition, drafting, execution and monitoring of complete migration plan for each of these use cases, in compliance with state of the art cryptographic algorithms, targeting achievement of migration of critical use cases by 2030 and medium and low level use cases by 2035; - Where the achievement of migration of use case can't be achieved in due time, a risk assessment and mitigation

#	Article	Original Text	Amendment	Rationale
				plan shall be defined, drafted and executed until the complete migration.
18.	Article 1(6)a (new) amending Article 21(2)(ja) (proposed point ja) of Directive (EU) 2022/2555	Article 21(2) does not address cybersecurity risks arising from excessive dependencies on cloud computing services, critical digital service providers, non-EU technologies or exposure to third-country laws affecting critical functions and data.	**Insert a new point (ja) in Article 21(2):** (ja) measures to identify and mitigate cybersecurity risks arising from excessive dependencies on cloud computing services and other critical digital service providers, including, where appropriate, measures aimed at ensuring an adequate level of resilience, control, continuity and recoverability of critical functions and data.	Essential and important entities increasingly rely on cloud computing services and remote data processing services to support the operation of critical functions and the processing of sensitive data. Such services may lead to excessive dependencies and create cybersecurity risks linked to the concentration of service providers, loss of operational control, reliance on non-Union technologies, or exposure to third-country laws and regulatory requirements. These risks may affect the confidentiality, integrity, availability or accessibility of systems and data. Cybersecurity risk-management measures should therefore explicitly include the assessment and mitigation of such dependencies. This would strengthen the resilience of essential and important entities and ensure greater consistency with other Union initiatives relating to cloud security, resilience and technological sovereignty, including the proposed Cloud and AI Development Act (CADA) and the European Cybersecurity Certification Scheme for Cloud Services (EUCS).
19.	Article 1(7) amemending Article 21(5) of	The proposal does not clarify the interaction between the new fifth subparagraph of Article	**Amendment to Article 21(5)(c) (new subparagraph)** The adoption of implementing acts pursuant to this paragraph shall be without prejudice to Article 24(1)	The proposed fifth subparagraph of Article 21(5) creates legal uncertainty regarding the interaction between implementing acts adopted under that provision and Article 24(1) of

#	Article	Original Text	Amendment	Rationale
	Directive (EU) 2022/2555	21(5) and Article 24(1) concerning cybersecurity certification requirements.	and to the possibility for Member States to require the use of ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881, or to maintain or introduce national cybersecurity certification or accreditation requirements where permitted under Union law.	Directive (EU) 2022/2555. In particular, it is unclear whether Member States would remain entitled to require essential and important entities to use ICT products, ICT services and ICT processes certified under European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 once an implementing act has been adopted. The proposal also creates uncertainty as to whether Member States could continue to maintain or introduce national cybersecurity certification or accreditation requirements, where permitted under Union law. Such schemes may play an important role in addressing specific cybersecurity needs and policy objectives at national level. For reasons of legal certainty and to ensure the coherent application of Articles 21 and 24 of Directive (EU) 2022/2555, it should be clarified that the adoption of implementing acts pursuant to Article 21(5) does not affect the powers granted to Member States under Article 24(1) or the possibility to maintain or introduce national certification or accreditation requirements where permitted under Union law.
20.	Article 1(7)(b) amemending Article 21(5) (proposed fifth	The proposal introduces a new fifth subparagraph prohibiting Member States from adopting or maintaining additional	**Delete the proposed fifth subparagraph of Article 21(5).**	The proposed fifth subparagraph would significantly alter the approach established by Directive (EU) 2022/2555 by preventing Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity where an

#	Article	Original Text	Amendment	Rationale
	subparagraph) of Directive (EU) 2022/2555	technical, methodological or sectoral cybersecurity requirements where an implementing act has been adopted.		implementing act has been adopted pursuant to Article 21(5). As a result, Member States would be limited to the technical, methodological and sectoral requirements laid down in those implementing acts. This would reduce the flexibility currently available to Member States under Article 5 to respond to their specific cybersecurity needs and priorities. In addition, cybersecurity requirements applicable to essential and important entities may be directly relevant to national security considerations, which remain the sole responsibility of each Member State. This will very likely result in levelling down the overall cybersecurity of important and essential entities throughout EU. Implementing acts laying down technical, methodological and sectoral requirements may apply to a wide range of entities covered by the Directive. Limiting Member States to the requirements set out in such implementing acts could reduce their ability to address specific cybersecurity risks, sectoral vulnerabilities or national priorities. Furthermore, cybersecurity requirements applicable to essential and important entities may be closely linked to national security considerations, which remain the sole responsibility of each Member State pursuant to Article 4(2) TEU.

#	Article	Original Text	Amendment	Rationale
				The Directive should therefore continue to allow Member States to adopt or maintain provisions ensuring a higher level of cybersecurity, in accordance with Union law.
21.	Article 1(7)(b)a (New) amending Article 21(5) (second subparagraph) of Directive (EU) 2022/2555	The proposal provides that, when preparing assessments under Article 21(5), the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.	**Add a third subparagraph to Article 21(5)** When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall consult the NIS Cooperation Group as well as relevant stakeholders in an open, transparent and inclusive manner.	Change to article 21.5 (change to the second paragraph) "[…] When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States." NIS directive has already established the NIS cooperation group. Due consideration shall be given to the NIS cooperation group when preparing such assessment. Therefore, the text should be changed as follows: "[…] When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall consult the NIS cooperation group as well as relevant stakeholders in an open, transparent and inclusive manner."
22.	Article 1(8) adding Article 23(12) of Directive (EU) 2022/2555	The proposal empowers the Commission to adopt implementing acts specifying additional information to be	**Delete the proposed Article 23(12).**	The proposed provision is unnecessary as it already predetermines the content of the implementing acts by specifying the information to be reported, namely whether a ransomware attack was detected, the attack

#	Article	Original Text	Amendment	Rationale
		submitted regarding ransomware attacks, while already identifying the information to be covered by those implementing acts.		vector, and whether mitigation measures have been implemented. For reasons of clarity and legal certainty, those requirements should be included directly in the Directive rather than left to a future implementing act.
23.	Article 1(8)a (new) amending Article 23(4) of Directive (EU) 2022/2555	Article 23(4) specifies the information to be submitted by entities when notifying incidents but does not include ransomware-specific information.	**Amend Article 23(4) by adding the following paragraph:** "The following information as regards ransomware attacks shall also be submitted:(a) whether the entity detected a ransomware attack;(b) the attack vector of the ransomware attack;(c) whether mitigation measures have been implemented."	The information identified by the Commission proposal is relevant and should be reported. Including these reporting requirements directly in Article 23(4) provides greater legal certainty, avoids unnecessary empowerment for future implementing acts and ensures that the applicable obligations are immediately clear to both reporting entities and competent authorities.
24.	Article 1(8)b (new) amending Article 23(4)(b) of Directive (EU) 2022/2555	Current NIS 2 requires entities to submit the incident notification referred to in Article 23(4)(b) within 72 hours of becoming aware of a significant incident. "without undue delay and in any event within **72**	**Amendment to Article 23(4)(b)** Replace with: "without undue delay and in any event within **96 hours** of becoming aware of the significant incident".	Data breaches and significant incidents on network and information security are usually correlated. When a significant incident occurs, it is also likely that it results in a data breach. Likewise, if an attacker aims at stealing data, it is likely to cause a significant incident. Therefore, to effectively reduce burden for Essential and Important Entities regarding their reporting obligations under NISD2 and GDPR, it is key that timelines for reporting incident

#	Article	Original Text	Amendment	Rationale
		hours of becoming aware of the significant incident"		notification and personal data breach are aligned under both NISD2 and GDPR. The proposal of Digital Omnibus (COM(2025) 837 final) amends the GDPR (article 33.1) regarding the timeline for reporting of personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons to move it from 72h to 96h. Therefore, to ensure overall consistency with the Digital Omnibus (COM(2025) 837 final), the timeline for notification in article 23.4(b) should be set to 96 hours (the current provision requires 72 hours).
25.	Article 1(8)c (new) amending Article 23(4) - last paragraph of Directive (EU) 2022/2555	The proposal requires trust service providers to notify significant incidents affecting the provision of their trust services without undue delay and, in any event, within 24 hours of becoming aware of the incident, while the general reporting deadline applicable to other entities is 72 hours.	**Delete the last paragraph of Article 23(4):** By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident. **And replace by:** **"By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without**	This exception - only applicable to "Non-qualified trust service providers" or "Qualified trust service providers" - implies that these entities are required to submit incident notifications without undue delay and in any event within 24 hours of becoming aware of the significant incident, while any other entities (which may also be Important Entities or Essential Entities) are only required to do so within 72 hours. This specific treatment for "Non-qualified trust service providers" or "Qualified trust service providers" is not explained nor supported by any recital within NISD2. This very short timeline creates huge constraints-entailing very substantial costs-only for "Non-qualified trust service providers" and

#	Article	Original Text	Amendment	Rationale
			undue delay and in any event within 24 hours of becoming aware of the significant incident."	"Qualified trust service providers" to meet this requirement. In line with the approach underpinning this amendment to NISD2 aiming at reducing "[…] the burden of compliance for entities and of supervision for competent authorities […]" (recital 2 and further reflected in the proposed new article 3.1(a)), the specific burden for "Non-qualified trust service providers" and "Qualified trust service providers" should thus be reduced in order to align it with the general rule. Therefore, this exception for "Non-qualified trust service providers" or "Qualified trust service providers" should be removed, so that such entities are subjects to the same timeline for incident reporting.
26.	Article 1(9) amending Article 24 (new paragraph 7) of Directive (EU) 2022/2555	The proposal does not provide a mechanism for recognising compliance with equivalent obligations under Regulation (EU) No 910/2014.	**Add a paragraph Article 24(7):** Where essential or important entities are subject to obligations under Regulation (EU) No 910/2014 which are equivalent to requirements laid down in this Directive, compliance with those obligations shall be taken into account for the purposes of demonstrating compliance with this Directive, in order to avoid duplication. Where an entity complies with obligations relating to security breach management, incident notification, reporting, certification or supervision under Regulation (EU) No 910/2014 that are equivalent to	The introduction of EUDIW and EBW providers within the scope of NIS2 creates potential overlaps with existing obligations under eIDAS. A mechanism recognising equivalent obligations and establishing a presumption of conformity would reduce administrative burden, avoid duplication and provide greater legal certainty for regulated entities and supervisory authorities.

#	Article	Original Text	Amendment	Rationale
			the requirements laid down in Articles 21, 23 or 24 of this Directive, that entity shall be presumed to comply with the corresponding requirements of this Directive to the extent that those obligations are equivalent. The Commission may, where appropriate, adopt implementing acts or issue guidelines specifying the application of this paragraph, including the identification of equivalent obligations under Regulation (EU) No 910/2014.	
27.	Article 1(9)a (new) amending Article 24(4) of Directive (EU) 2022/2555	The proposal refers to Article 75 of Regulation (EU) XXX/XXX [Proposal for CSA2] as the legal basis for European cybersecurity certification schemes on the cyber posture of entities.	**Amend Article 24(4) as follows:** In order to demonstrate compliance with Article 21, Member States may require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX [Proposal for CSA2].	The reference to Article 75 of the Proposal for a Regulation amending Regulation (EU) 2019/881 (CSA2) is incorrect. The relevant legal basis for the adoption of European cybersecurity certification schemes is Article 74. The reference should therefore be corrected to ensure legal accuracy and consistency with the CSA2 proposal.
28.	Article 1(9)b (new) adding Article 24 (7) of Directive (EU) 2022/2555	The proposal introduces a mechanism allowing entities to demonstrate compliance with Article 21 through a certificate on the cyber posture under a European cybersecurity certification scheme	**Amend Article 1(9) as follows:** In Article 24, the following paragraphs 4, 5, 6 **and 7** are added: […] 7. **When preparing European cybersecurity certification schemes referred to in this Article, the Commission shall, where appropriate, consult the NIS Cooperation Group competent supervisory authorities, industry, essential and important entities."**	The effectiveness, usability and acceptance of European cybersecurity certification schemes on the cyber posture of entities will depend on the involvement of the stakeholders responsible for implementing, assessing, supervising and relying upon them. The preparation of such schemes should therefore benefit from the expertise of the NIS Cooperation Group, competent supervisory authorities, industry representatives, and essential and important entities. Explicit consultation of these stakeholders would improve the quality, practicality and consistency of the schemes and

#	Article	Original Text	Amendment	Rationale
				facilitate their adoption and implementation across the Union.
29.	Article 1(11)(a) amending Article 27(1) of Directive (EU) 2022/2555	The proposal establishes an ENISA registry covering essential and important entities.	**Amendment to Article 27(1)** Replace the proposed text with: ENISA shall establish and maintain a registry containing information on essential and important entities where such information is necessary for the performance of the tasks entrusted to ENISA under this Directive. The registry shall be limited to entities providing services in more than one Member State and to other entities where the inclusion of such information is necessary to support cooperation, mutual assistance or other tasks provided for under this Directive. Competent authorities shall have access to the information contained in the registry where necessary for the exercise of their responsibilities under this Directive.	The necessity of maintaining a comprehensive Union-level registry containing information on all essential and important entities has not been demonstrated. Information stored in this registry concerning most entities will not be accessible to competent authorities. An exception is introduced for some types of entities for which competent authorities would be allowed to access information stored in that registry: DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers. Nevertheless, for most of entities described in Annex I and Annex II of NISD2, competent authorities would not be allowed to access information stored in that registry concerning them. **Therefore, introducing a registry of essential and important entities for which most of the information could not be accessed by any competent authorities nor used by any entities seems useless.**

#	Article	Original Text	Amendment	Rationale
30.	Article 1(11)(c) amending Article 27(4) of Directive (EU) 2022/2555	The proposal requires Member States to transmit information to the ENISA registry.	**Amendment to Article 27(4)** Replace the proposed text with: *Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall transmit to ENISA the information necessary for the purposes of paragraph 1. Member States may, in duly justified cases and in particular where national security considerations are involved, limit or refrain from transmitting specific information where they consider that such transmission would adversely affect their essential national security interests.*	**This information is very sensitive in nature**. Gathering all this information into a single central registry managed by ENISA would create a **very interesting target for cyberattacks, as hacking that single central registry would allow threat actors to get all information about important and essential entities within all the Member State.** Therefore, in **order to mitigate risks stemming from cyber-attacks on this very sensitive information, the establishment of a single central repository should be avoided.** Instead, the current setting should be kept, whereby each Member State maintains its own registry. As such, to get all information about important and essential entities within all the Member State, threat actors would have to hack 27 different IT systems with different and various IT security. **Therefore, a registry of important and essential entities maintained by ENISA should not be established.** In addition, **considering that cybersecurity of important and essential entities is also directly relevant for national security (which is not a EU competency but a national competency), it shall be possible for MS not to communicate the list of its important and essential entities to another stakeholder (ENISA)**.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com