Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA comments on the NIS Directive consultation

1 October 2020

Section 1: General questions on the NIS Directive

Sub-section 1.a. – Relevance of the NIS Directive

The NIS Directive envisages to (1) increase the capabilities of Member States when it comes to mitigating cybersecurity risks and handling incidents, (2) improve the level of cooperation amongst Member States in the field of cybersecurity and the protection of essential services, and (3) promote a culture of cybersecurity across all sectors vital for our economy and society.

Q1: To what extent are these objectives still relevant?

	Not relevant at all	Not relevant	Relevant	Very relevant	Don't know / no opinion
Increase the capabilities of Member States				X	
Improve the level of cooperation amongst Member States				X	
Promote a culture of security across all sectors vital for our economy and society				X	

Sub-section 1.b. – Cyber-threat landscape

Q1: Since the entry into force of the NIS Directive in 2016, how has in your opinion the cyber threat landscape evolved?

- ❏ Cyber threat level has decreased significantly
- ❏ Cyber threat level has decreased
- ❏ Cyber threat level is the same

- ✓ **Cyber threat level has increased**
- ❑ Cyber threat level has increased significantly
- ❑ Don't know / no opinion

Q2: How do you evaluate the level of preparedness of small and medium-sized companies in the EU against current cyber threats (on a scale from 1 to 5 with 5 indicating that companies score highly on cyber resilience)?

- ❑ 1
- ❑ 2
- ❑ 3
- ❑ 4
- ❑ 5
- ❑ Don't know / no opinion

Sub-section 1.c. – Technological advances and new trends

Technological advances and new trends provide great opportunities to the economy and society as a whole. The growing importance of edge computing (which is a new model of technology deployment that brings data processing and storage closer to the location where it is needed, to improve response times and save bandwidth), as well as the high reliance on digital technologies especially during the COVID-19 crisis increases at the same time the potential attack surface for malicious actors. All this changes the paradigm of security resulting in new challenges for companies to adapt their approaches to ensuring the cybersecurity of their services.

Q1: In which way should such recent technological advances and trends be considered in the development of EU cybersecurity policy?

1000 character(s) maximum

Sub-section 1.d. – Added-value of EU cybersecurity rules

The NIS Directive is based on the idea that common cybersecurity rules at EU level are more effective than national policies alone and thus contribute to a higher level of cyber resilience at Union level.

Q1: To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Cyber risks can propagate across borders at high speed, which is why cybersecurity rules should be aligned at Union level				X	
The mandatory sharing of cyber risk related information between national authorities across Member States would contribute to a higher level of joint situational awareness when it comes to cyber risks					X
All entities of a certain size providing essential services to our society should be subject to similar EU-wide cybersecurity requirements			X		

Sub-section 1.e. – Sectoral scope

Under the current NIS Directive, certain public and private entities are required to take appropriate security measures and notify serious incidents to the relevant national authorities. Entities subject to these requirements include so-called operators of essential services (OES) and digital service providers (DSP).

Operators of essential services are entities operating in seven sectors and subsectors: energy (electricity, oil and gas), transport (air, rail, water and road), banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure (IXPs, DNS providers and TLD registries). Digital service providers are either cloud service providers, online search engines or online marketplaces.

Q1: Should the following sectors or services be included in the scope of the Directive due to their exposure to cyber threats and their importance for the economy and the society as a whole?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Public administration					X
Food supply					X
Manufacturing	X				
Chemicals					X
Waste water					X
Social networks	X				
Data centres	X				

Q2: Should undertakings providing public communications networks or publically available electronic communications services currently covered by the security and notification requirements of the EU telecom framework be included in the scope of the NIS Directive?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Q3: Do you consider that also other sectors, subsectors and/or types of digital services need to be included in the scope of the Directive due to their exposure to cyber threats and their importance for the economy and the society as a whole?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Sub-section 1.f. – Regulatory treatment of OES and DSPs by the NIS Directive

As regards the imposition of security and notification requirements, the NIS Directive distinguishes between two main categories of economic entities: operators of essential services (OES) and digital service providers (DSP). While in the case of OES, Member States are allowed to impose stricter security and notification requirements than those enshrined in the Directive, they are prohibited to do so for DSPs. Moreover, competent authorities can only supervise DSPs "ex-post" (when an authority is provided with evidence that a company does not fulfil its obligations) and not "ex-ante" as in the case of OES. These are elements of the so-called "light-touch" regulatory approach applied towards DSPs, which was

motivated by the lower degree of risk posed to the security of the digital services and the cross-border nature of their services.

Q1: Do you agree that the "light-touch" regulatory approach applied towards DSPs is justified and therefore should be maintained?

- ✓ **Yes**
- ❑ No
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

More prescriptive requirements and invasive local oversight for essential services are justified, particularly for those OES which operate in only one jurisdiction. This is not necessary for services provided by DSPs which are providing their services across multiple jurisdictions, within and outside the European Union.

Equating DSPs to OES would also create practical implementation challenges given the diversity of DSPs currently in scope. The sheer burden of the obligations on operators will inevitably affect competent authorities' capabilities to enforce those obligations, and the overall effectiveness, strength, and agility of the EU's future cybersecurity framework.

The implementation experience of the NIS Directive is still relatively new for many actors, from DSPs, OES and their suppliers, to national competent authorities. This review should focus on improving the existing framework and resolving the shortcomings of its implementation rather than expanding its scope.

Sub-section 1.g. – Information sharing

Under the NIS Directive, Member States must require operators of essential services (OES) and digital service providers (DSP) to report serious incidents. According to the Directive, incidents are events having an actual adverse effect on the security of network and information systems. As a result, reportable incidents constitute only a fraction of the relevant cybersecurity information gathered by OES and DSPs in their daily operations.

Q1: Should entities under the scope of the NIS Directive be required to provide additional information to the authorities beyond incidents as currently defined by the NIS Directive?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Section 2: Functioning of the NIS Directive

Sub-section 2.a. – National strategies

The NIS Directive requires Member States to adopt national strategies on the security of network and information systems defining strategic objectives and policy measures to achieve and maintain a high level of cybersecurity and covering at least the sectors referred to in Annex II and the services referred to in Annex III of the Directive.

Q1: In your opinion, how relevant are common objectives set on EU level for the adoption of national strategies on the security of network and information systems in order to achieve a high level of cybersecurity?

- ❑ Not relevant at all
- ❑ Not relevant
- ✓ **Relevant**
- ❑ Very relevant
- ❑ Don't know / no opinion

Q2: Taking into account the evolving cybersecurity landscape, should national strategies take into account any additional elements so far not listed in the Directive?

- ❑ Yes
- ❑ No
- ❑ Don't know / no opinion

Sub-section 2.b. – National competent authorities and bodies

The Directive requires Member States to designate one or more national competent authorities on the security of network and information systems to monitor the application of the Directive on a national level. In addition, Member States are required to appoint a single point of contact to ensure cross-border cooperation with the relevant authorities in other Member States and with the Cooperation Group and the CSIRT network as well as one or more computer security incident response teams (CSIRTs) responsible for risk and incident handling for the sectors and services covered by Annex II and III of the Directive.

Q1: In your opinion what is the impact of the NIS Directive on national authorities dealing with the security of network and information systems in the Member States?

	No impact	Low impact	Medium impact	High impact	Don't know / no opinion

Level of funding					X
Level of staffing					X
Level of expertise					X
Cooperation of authorities across Member States		X			
Cooperation between national competent authorities within Member States					X

Q2: In your opinion, what is the impact of the NIS Directive on national Computer Security Incident Response Teams (CSIRTs) in the Member States?

	No impact	Low impact	Medium impact	High impact	Don't know / no opinion
Level of funding					X
Level of staffing					X
Level of operational capabilities					X
Level of expertise					X
Cooperation with OES and DSP			X		
Cooperation with relevant national competent authorities (such as sectoral authorities)			X		

Q3: How do you evaluate the quality of services provided by the national Computer Security Incident Response Teams to OES (on a scale from 1 to 5 with 5 indicating a very high level of quality)?

- ❑ 1
- ❑ 2
- ✓ 3
- ❑ 4
- ❑ 5

- ❑ Don't know / no opinion

Q4: How do you evaluate the quality of services provided by the national Computer Security Incident Response Teams to DSPs (on a scale from 1 to 5 with 5 indicating a very high level of quality)?

- ❑ 1
- ✓ **2**
- ❑ 3
- ❑ 4
- ❑ 5
- ❑ Don't know / no opinion

Q5: Under the NIS Directive, competent authorities or the CSIRTs shall inform the other affected Member State(s) if an incident has a significant impact on the continuity of essential services in that Member State. How do you evaluate the level of incident-related information sharing between Member States (on a scale from 1 to 5 with 5 indicating a very high degree of satisfaction with the information shared)?

- ❑ 1
- ✓ **2**
- ❑ 3
- ❑ 4
- ❑ 5
- ❑ Don't know / no opinion

Q6: If you are an OES/DSP: Has your organisation received technical support from the national CSIRTs in case of an incident?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Q7: Should the CSIRTs be assigned additional tasks so far not listed in the NIS Directive?

- ✓ **Yes**
- ❑ No
- ❑ Don't know / no opinion

If yes, please specify which tasks:
500 character(s) maximum

CSIRTs may act as the SPOC for all providers of cross-border services under a one-stop-shop mechanism, for both DSPs and OES (e.g. digital infrastructures). See our recommendations for a one-

stop-shop-mechanism for cross-border essential services further below.

Q8: How do you evaluate the functioning of the single points of contact (SPOCs) since their establishment by the NIS Directive as regards the performance of the following tasks (on a scale from 1 to 5 with 5 indicating a very high level of performance)?

	1	2	3	4	5	Don't know / no opinion
Cross-border cooperation with the relevant authorities in other Member States						
Cooperation with the Cooperation Group						
Cooperation with the CSIRTs network						

Q9: Should the single points of contact be assigned additional tasks so far not listed in the NIS Directive?

- ✓ **Yes**
- ❑ No
- ❑ Don’t know / no opinion

If yes, please specify which tasks:
500 character(s) maximum

See answer to question 7.

Q10: How do you evaluate the level of consultation and cooperation between competent authorities and SPOCs on the one hand, and relevant national law enforcement authorities and national data protection authorities on the other hand (on a scale from 1 to 5 with 5 indicating a very high level of cooperation)?

- ❑ 1
- ❑ 2
- ❑ 3
- ❑ 4
- ❑ 5
- ❑ Don’t know / no opinion

Sub-section 2.c. – Identification of operators of essential services and sectoral scope

Operators of essential services are organisations that are important for the functioning of the economy and society as a whole. While the NIS Directive provides a list of sectors and subsectors, in which particular types of entities could become subject to security and incident reporting requirements, Member States are required to identify the concrete operators for which these obligations apply by using criteria set out in the Directive.

Q1: To what extent do you agree with the following statements regarding the concept of identification of operators of essential services (OES) introduced by the NIS Directive and its implementation by Member States?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The current approach ensures that all relevant operators are identified across the Union.		X			
OES are aware of their obligations under the NIS Directive.		X			
Competent authorities actively engage with OES.					X
The cross-border consultation procedure in its current form is an effective element of the identification process to deal with cross-border dependencies.		X			
The identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States.		X			

Please elaborate your answer:

1000 character(s) maximum

Today, an undertaking providing a service in several Member States can be treated as an OES in one Member State, a DSP in another Member State, or a service provider falling out of the NIS Directive in yet a different Member State. Existing convergence tools (i.e. Article 5(4) consultation procedure, and the NIS Cooperation Group working document on the identification of OES) have not been sufficiently used to achieve consistent identification or OES across the Union. This is a problem for companies operating in multiple jurisdictions and it undermines the functioning of the internal market.

In this respect, the European Commission's OES identification report broadly reflects some of our Members' hands-on experience in different national markets, particularly with respect to "Digital Infrastructure" services such as DNS.

Q2: Given the growing dependence on ICT systems and the internet in all sectors of the economy, to what extent do you agree with the following statements regarding the scope of the NIS Directive when it comes to operators of essential services?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Definitions of the types of entities listed in Annex II are sufficiently clear.		X			
More sectors and sub-sectors should be covered by the Directive.					X
Identification thresholds used by Member States should be lower (i.e. more companies should be covered).					X

Please elaborate your answer:

1000 character(s) maximum

We refer to our answer to the previous question.

Q3: If you agree with the statement above that more sectors and sub-sectors should be covered by the Directive, which other sectors should be covered by the scope of the NIS Directive and why?

Please elaborate your answer:

1000 character(s) maximum

CCIA believes that the on-going review of the NIS Directive should primarily focus on improving the existing framework and harmonizing the implementation and enforcement of the rules for all cross-border services. Broadening the scope of the directive to additional sectors would require extensive risk-based assessment. Market players which are already subject to cybersecurity requirements in sector-specific legislation must remain excluded from the scope of the Directive. Additional sectors should only be contemplated where there is factual evidence of cybersecurity lack of preparedness, increase of risks, and a demonstrable regulatory gap in a given sector.

Q4: How has the level of risk of cyber incidents in the different sectors and subsectors covered by the NIS Directive evolved since the Directive entered into force in 2016?

	Very significant decrease in risk	Significant decrease in risk	No increase or decrease in risk	Significant increase in risk	Very significant increase in risk	Don't know / no opinion
Electricity					X	
Oil					X	
Gas					X	
Air transport					X	
Rail transport			X			
Water transport			X			
Road transport				X		
Banking					X	
Financial market infrastructures					X	
Health sector					X	
Drinking water supply and distribution			X			

Digital infrastructure (IXPs,DNS providers, TLD registries)			X			

Q5: How do you evaluate the level of cybersecurity resilience when it comes to the different sectors and subsectors covered by the NIS Directive?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Electricity		X				
Oil				X		
Gas				X		
Air transport				X		
Rail transport		X				
Water transport		X				
Road transport			X			
Banking					X	
Financial market infrastructures					X	
Health sector	X					
Drinking water supply and distribution		X				
Digital infrastructure (IXPs,DNS providers, TLD registries)					X	

Q6: How do you evaluate the level of cyber resilience and the risk-management practices applied by those small and medium-sized companies that are not covered by the NIS Directive (on a scale from 1 to 5 with 5 indicating that companies score highly on cyber resilience)?

	1	2	3	4	5	Don't know / no opinion
Small companies						

Medium-sized companies						

Please elaborate your answers for both small and medium-sized companies:

	Your elaboration
Small companies	
Medium-sized companies	

Q7: Do you think that the level of resilience and the risk-management practices applied by companies differ from sector to sector for small and medium-sized companies?

- ❏ Yes
- ❏ No
- ✓ **Don't know / no opinion**

If yes, please elaborate your answer:

1000 character(s) maximum

Sub-section 2.d. – Digital service providers and scope

Digital service providers (cloud service providers, online search engines and online marketplaces) shall also put in place security measures and report substantial incidents. For this type of entities, the Directive envisages a "light-touch" regulatory approach, which means inter alia that competent authorities can only supervise DSPs "ex-post" (when an authority is provided with evidence that a company does not fulfil its obligations). Member States are not allowed to impose any further security or reporting requirements than those set out in the Directive ("maximum harmonisation"). Jurisdiction is based on the criterion of main establishment in the EU.

Q1: To what extent do you agree with the following statements regarding the way in which the NIS Directive regulates digital service providers (DSPs)?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Annex III of the NIS				X	

Directive covers all relevant types of digital services.					
Definitions of the types of digital services listed in Annex III are sufficiently clear.			X		
Competent authorities have a good overview of the DSPs falling under their jurisdiction.			X		
Competent authorities actively engage with DSPs under their jurisdiction.			X		
Security requirements for DSPs are sufficiently harmonised at EU level.			X		
Incident notification requirements for DSPs are sufficiently harmonised at EU level.			X		
Reporting thresholds provided by the Implementing Regulation laying down requirements for Digital Service Providers under the NIS Directive are appropriate.			X		

Q2: If you disagree with the statement above that Annex III of the NIS Directive covers all relevant types of digital services, which other types of providers of digital services should fall under the scope of the NIS Directive and why ?

1000 character(s) maximum

Q3: To what extent do you agree with the following statements regarding the so-called “light-touch approach” of the NIS Directive towards digital service providers (DSPs)?

	Strongly disagree	Disagree	Agree	Strongly Agree	Don't know / no opinion
The more harmonised regulatory approach applied towards DSPs as compared to OES is justified by the cross-border nature of their services.				X	
Subjecting DSPs to the jurisdiction of the Member State where they have their main establishment in the EU minimises the compliance burden for those companies.				X	
The limitation related to the supervisory power of the national authorities, notably to take action only when provided with evidence (ex-post supervision), in the case of the DSPs is justified by the nature of their services and the degree of cyber risk they face.				X	
The exclusion of micro- and small enterprises is reasonable considering the limited impact of their services on the economy and society as a whole.					X

Please elaborate your answer:

1000 character(s) maximum

Most digital services ("DSPs") and network services ("OES/digital infrastructures" such as DNS) are provided uniformly across the EU's internal market, without prejudice to specific customer requirements. Substantive and enforcement cybersecurity rules should reflect the cross-border nature of those services, such as is the case with the one-stop-shop and single point of contact mechanisms under the NIS Directive.

CCIA supports this kind of practical mechanism as it ensures (1) consistent regulatory enforcement across the internal market, (2) seamless and timely communications between a DSP and a single authority in time-sensitive incident scenarios. (3) It also puts less constraints on regulatory authorities' enforcement and DSPs' compliance resources.

Q4: How do you evaluate the level of preparedness of digital service providers covered by the NIS Directive when it comes to cybersecurity related risks?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Online marketplaces					X	
Online search engines					X	
Cloud computing services					X	

Q5: In the previous question, you have been asked about the level of preparedness of different types of digital service providers. Please explain your assessment of the level of preparedness:

	Your elaboration
Online marketplaces	**Robust cybersecurity policies and measures are put in place and are periodically reviewed to adapt to a changing cybersecurity threat landscape. They apply to both (existing and new) customer-facing products as well as internal / third party systems. Detailed contractual arrangements govern third party vendors' security and incident reporting obligations.**
Online search engines	**Robust cybersecurity policies and measures are put in place and are periodically reviewed to adapt to a changing cybersecurity threat landscape. They apply to both (existing and new) customer-facing products as well as internal infrastructures.**
Cloud computing services	**Robust cybersecurity policies and measures are put in place and are periodically reviewed to adapt to a changing cybersecurity threat landscape. These apply to both**

	(existing and new) customer-facing products as well as internal / third party systems. Detailed contractual arrangements govern third party vendors' security and incident reporting obligations.

Q6: How has the level of risk of cyber incidents in the different sectors and subsectors covered by the NIS Directive evolved since the Directive entered into force in 2016?

	Very significant decrease in risk	Significant decrease in risk	No increase or decrease in risk	Significant increase in risk	Very significant increase in risk	Don't know / no opinion
Online marketplaces			**X**			
Online search engines			**X**			
Cloud computing services				**X**		

Q7: How do you evaluate the level of cybersecurity resilience when it comes to the different types of digital service providers covered by the NIS Directive?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Online marketplaces					**X**	
Online search engines					**X**	
Cloud computing services					**X**	

Sub-section 2.e. – Security requirements

Member States are required to ensure that entities take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems.

Q1: What is the impact of imposing security requirements on OES by the NIS Directive in terms of cyber resilience?

- ❑ No impact
- ❑ Low impact
- ✓ **Medium impact**

- ❑ High impact
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

The NIS Directive provides a common, principle-based baseline for OES to implement technical and organisational security measures in all Member States.

CCIA observes vast differences in the way Member States have implemented OES security requirements under the NIS Directive, as well as the scope of OES and thresholds of criticality. While the fragmentation of national security requirements does not raise concerns for OES operating in a single Member State, different security requirements may raise implementation and compliance conflicts for providers of essential services operating in several Member States or globally (such as some DNS services).

Q2: What is the impact of imposing security requirements on DSPs by the NIS Directive in terms of cyber resilience?

- ❑ No impact
- ❑ Low impact
- ✓ **Medium impact**
- ❑ High impact
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Consistent with our response to questions 4 and 5 of subsection 2.d, DSPs tend to have a very high level of cybersecurity preparedness. By their very nature, DSPs are acutely aware of the cybersecurity threat landscape and have a track-record of designing security risk mitigation and contingency measures for their own and enterprise customers' services. The NIS Directive has codified existing industry practices.

CCIA notes that the fragmented implementation of security requirements for OES also has knock-on effects on third-party DSPs.

Q3: To what extent do you agree with the following statements regarding the implementation of security requirements under the NIS Directive?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Member States have established effective security requirements for OES on a national level.		X			
There is a sufficient degree of alignment of security requirements for OES and DSPs in all MS.					X

Please elaborate your answer:

1000 character(s) maximum

OES have distinct, granular, and sometimes prescriptive security requirements from one Member States to another, unlike most DSPs. While this may suit OES operating in only one Member State, this creates inefficiencies for:
(a) providers of cross-border essential services (e.g. digital infrastructures, DNS)
(b) providers of cross-border digital services which offer their services to OES and which the national competent authority deems essential for the maintenance of critical societal and economic activities. Harmonisation of security requirements and a One-Stop-Shop are essential for those services.

As to the second question, and consistent with our previous answers, CCIA does not believe that DSPs and OES should bear the same security requirements. As mentioned before, OES are subject to specific national requirements (including certifications) which does not suit DSPs' cross-border services.

Are there sectoral differences for OES regarding how effectively security requirements have been put in place by the Member States?

- ✓ **Yes**
- ❑ No
- ❑ Don't know / no opinion

Q4: While some Member States have put in place rather general security requirements, other Member States have enacted very detailed requirements featuring a higher degree of prescriptiveness. To what extent do you agree with the following statements regarding these different approaches?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion

Prescriptive requirements make it easy for companies to be compliant.		X			
Prescriptive requirements leave too little flexibility to companies.			X		
Prescriptive requirements ensures a high level of cybersecurity.		X			
Prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments.				X	
The different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets.				X	
The companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements.			X		
The companies should be required to use certification for their compliance with NIS security requirements.	X				

Please elaborate your answer:

1000 character(s) maximum

As a general comment, the more prescriptive and granular the requirements, the more static and the more likely they address past and present security risks. Prescriptive requirements might therefore be less effective to identify and mitigate cybersecurity risks in the long run. Principle-based requirements leave organisations the necessary flexibility to adapt to the evolving cybersecurity threat landscape and technological change.

CCIA believes that security requirements should drive organisations' accountability vis-a-vis their competent authorities and serve as one of the tools to measure up an organisation's cybersecurity measures against a dynamic cybersecurity benchmark.

Sub-section 2.f. – Incident notification

Member States are required to ensure that entities notify the competent authority or the CSIRT of incidents having a significant impact on the continuity or provision of services.

Q1: To what extent do you agree with the following statements regarding the implementation of notification requirements under the NIS Directive?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The majority of companies have developed a good understanding of what constitutes an incident that has to be reported under the NIS Directive.			X		
Member States have imposed notification requirements obliging companies to report all significant incidents.		X			
Different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES.				X	

The current approach ensures that OES across the Union face sufficiently similar incident notification requirements.	X				

Please elaborate your answer:

1000 character(s) maximum

Cross-border OES services are subject to different incident requirements and procedures. For example, notifications should be done by simple email in some Member States while others request OES to provide information through form submission or even document uploads. The deadline for reporting incidents also varies from one Member State to another.

More generally, the reporting of incidents is of secondary importance to procedures and technologies for finding, responding and remediating an incident. The impact of the cyber security posture of OES would be higher if NIS controls were developed to focus on establishing *proactive* measures, such as incident detection and response. In practice this means services such as comprehensive threat hunting, automated asset inventory, vulnerability management and configuration control delivered in the form of alerts, audit trails and automated reports.

Sub-section 2.g. – Level of discretion on transposition and implementation given to Member States

The NIS Directive gives a wide room of discretion to Member States when it comes to the identification of operators of essential services, the setting of security requirements and the rules governing incident notification.

Q1: To what extent do you agree with the following statements regarding this approach from an internal market perspective?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The approach leads to significant differences in the application of the Directive and has a strong negative impact				X	

on the level playing field for companies in the internal market.					
The approach increases costs for OES operating in more than one Member State.				X	
The approach allows Member States to take into account national specificities.			X		

Please elaborate your answer:

1000 character(s) maximum

We recognise that Member States should have a margin of discretion to oversee the network and information security practices of strictly national essential service providers. However, the fragmentation of incident reporting and security requirements is ill-suited for essential services which are provided in several Member States.

CCIA believes the on-going review process is an opportunity to harmonise the enforcement and oversight framework for cross-border essential services and introduce a One-Stop-Shop mechanism akin to the framework applicable to DSPs under Article 16(6) and Article 17(3).

Sub-section 2.h. – Enforcement

The Directive requires Member States to assess the compliance of operators of essential services with the provisions of the Directive. They must also ensure that competent authorities act when operators of essential services or digital service providers do not meet the requirements laid down in the Directive. Member States must also lay down rules for penalties that are effective, proportionate and dissuasive.

Q1: To what extent do you agree with the following statements regarding national enforcement of the provisions of the NIS Directive and its respective national implementations?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Member States are effectively enforcing the compliance of OES.			X		

Member States are effectively enforcing the compliance of DSPs.			X		
The types and levels of penalties set by Member States are effective, proportionate and dissuasive.			X		
There is a sufficient degree of alignment of penalty levels between the different Member States.					X

Sub-section 2.i. – Information exchange

The NIS Directive has created two new fora for information exchange: the Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs network, which promotes swift and effective operational cooperation between national CSIRTs.

Q1: To what extent do you agree with the following statements regarding the functioning of the Cooperation Group and the CSIRTs network?

	Strongly disagree	Disagree	Agree	Strongly disagree	Don't know / no opinion
The Cooperation Group has been of significant help for the Member States to implement the NIS Directive.					
The Cooperation Group has played an important role in aligning national transposition measures.					
The Cooperation Group has been instrumental in dealing					

with general cybersecurity matters.					
The Cooperation Group is dealing with cross-border dependencies in an effective manner.					
The CSIRTs network has effectively managed to fulfil its tasks as laid down in the NIS Directive.					
The CSIRTs network has helped to build confidence and trust amongst its members.					
The CSIRTs network has achieved swift and effective operational cooperation.					
The Cooperation Group and the CSIRTs network cooperate effectively.					

Q2: Should the Cooperation Group be assigned additional tasks so far not listed in the NIS Directive?

- ✓ **Yes**
- ❑ No
- ❑ Don't know / no opinion

If yes please specify which tasks:

500 character(s) maximum

The Cooperation Group may have a role to play when implementing and enforcing a one-stop-shop mechanisms for cross-border essential services and harmonisation of security requirements.

Q3: Should the CSIRTs network be assigned additional tasks so far not listed in the NIS Directive?

- ✓ **Yes**

- ❑ No
- ❑ Don't know / no opinion

Sub-section 2.j. – Efficiency of the NIS Directive

Q1: To what extent have the effects of the NIS Directive been achieved at a reasonable cost? To what extent are the costs of the intervention justified and proportionate given the benefits it has achieved?

- ❑ Not at all
- ❑ To a little extent
- ✓ **To some extent**
- ❑ To a large extent
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

The cost varies between the type of service providers. OES providing cross-border services bear the greatest compliance burden as they have to comply with different national security and reporting requirements and procedures. This is an unnecessary cost which diverts resources to pure compliance for the sake of compliance, with little to no results in achieving greater cyber resilience for companies. This can be mitigated through greater harmonisation and the introduction of a one-stop-shop.

Q2: What impact has the NIS Directive had on the overall level of resilience against cyber-threats across the EU when it comes to entities providing services that are essential for the maintenance of critical societal and economic activities?

- ❑ No impact
- ❑ Low impact
- ✓ **Medium impact**
- ❑ High impact
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

See the answer to the question above.

Sub-section 2.k. – Coherence of the NIS Directive with other EU legal instruments

The NIS Directive is not the only legal instrument on EU level that seeks to ensure more security of our digital environment. EU laws such as the General Data Protection Regulation or the European Electronic Communications Code are pursuing similar objectives.

Q1: To what extent are the provisions of the NIS Directive (such as on security requirements and incident notification) coherent with the provisions of other EU legal instruments that are aimed at increasing the level of data protection or the level of resilience?

- ❑ 1
- ✓ **2**
- ❑ 3
- ❑ 4
- ❑ 5
- ❑ Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

The NIS Directive is broadly coherent with other relevant EU legislation aimed at increasing the level of data protection or the level of resilience.

However, the national implementation of the NIS Directive has often created inconsistencies and conflicts with other relevant EU legislation. For instance, Cyprus, Estonia and Slovakia have enlisted *electronic communications services* (ECS) as OES. It is unclear how national NIS requirements of ECS providers meet Articles 40 and 41 of the Electronic Communications Code.

CCIA supports efforts to harmonise rules on incident reporting for DSPs across Member States and to achieve consistency with other applicable national and European reporting frameworks.

Section 3: Approaches to cybersecurity in the European context currently not addressed by the NIS Directive

Sub-section 3.a. – Provision of cybersecurity information

Pursuant to the provisions of NIS Directive, Member States have to require operators of essential services and digital service providers to report incidents above certain thresholds. However, organisations collect a lot of valuable information about cybersecurity risks that do not materialise into reportable incidents.

Q1: How could organisations be incentivised to share more information with cybersecurity authorities on a voluntary basis?

1000 character(s) maximum

CCIA believes CSIRTs and cyber agencies need a wider view of the threats. Probing near misses could improve threat intelligence, but this should be undertaken on a voluntary basis with a clear definition of a "near miss".

As regards vulnerability disclosure, this should be limited to government information sharing with the industry. Otherwise CSIRTs would be inundated with information e.g. the reporting of thousands of patch misconfigurations is not helpful. Further, consideration should be given to how existing mechanisms (including through CSIRTs) could be better leveraged and aligned with the regulatory reporting regimes. In any case, separating regulatory functions from CSIRTs – which is not the case in all Member States – is paramount.

Q2: Under the NIS Directive, Member States shall require companies to report events having an actual adverse effect on the security of network and information systems (incidents). Should the reporting obligations be broadened to include other types of information in order to improve the situational awareness of competent authorities?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Q3: The previous two questions have explored ways of improving the information available to cybersecurity authorities on national level. Which information gathered by such authorities should be made available on European level to improve common situational awareness (such as incidents with cross-border relevance, statistical data that could be aggregated by a European body etc.)?

1000 character(s) maximum

CCIA believes better information sharing between and amongst CSIRTs is of critical importance in the NIS review. CSIRTs need to be able to consume more threat intelligence feeds, widening the visibility, providing greater insights to their stakeholders and making their intelligence more actionable. ENISA has played a constructive role in facilitating information exchange, but we believe that more can be done. CSIRTs need their APIs to be interoperable with other threat intelligence information feeds and many of them currently lack good processes to consume threat intelligence. We think ENISA could play a valuable role in improving threat intelligence consumption through greater automation and interoperability between feeds.

Sub-section 3.b. – Information exchange between companies

Some Member States have fostered the development of fora where companies can exchange information about cybersecurity. This includes inter alia public private partnerships (PPP) or sectorial Information Sharing and Analysis Centres (ISACs). To some extent, such fora also exist on European and international level.

Q1: How would you evaluate the level of information exchange between organisations in their respective sectors when it comes to cybersecurity?

	Very low level	Low level	Medium level	High level	Very high level	Don't know / no opinion
Electricity						X
Oil						X
Gas						X
Air transport						X
Rail transport						X
Water transport						X
Road transport						X
Banking						X
Financial market infrastructures						X
Health sector						X
Drinking water supply and						X

distribution						
Digital infrastructure (IXPs,DNS providers, TLD registries)					X	
Digital service providers (online marketplaces)					X	
Digital service providers (online search engines)					X	
Digital service providers (cloud computing services)					X	

Q2: How would you evaluate the level of information exchange between organisations across sectors when it comes to cybersecurity?

- ❑ Very low level
- ❑ Low level
- ✓ **Medium level**
- ❑ High level
- ❑ Very high level
- ❑ Don't know / no opinion

Q3: How could the level of information exchange between companies be improved within Member States but also across the European Union?

1000 character(s) maximum

CCIA invites the European Commission to consider further encouraging direct sharing between companies without involving national authorities. In practice, there may be circumstances where a company may have specific indicators of compromises that it is appropriate for them to share with other companies.

To do so, we encourage the European Commission to consider providing companies with greater comfort with how information sharing can be conducted without unduly exposing their liability under the GDPR and e-Privacy framework. The revised NIS framework should put less risk on those companies adopting these practices in good faith. For instance, specific exemptions would be preferable to a reliance on legitimate interest. The European Commission could also create approved frameworks which, if used, can be considered prima facie evidence of compliance.

Sub-section 3.c. – Vulnerability discovery and coordinated vulnerability disclosure

While the negative impact of vulnerabilities present in ICT products and services is constantly increasing, finding and remedying such vulnerabilities plays an important role in reducing the overall cybersecurity risk. Cooperation between organisations, manufacturers or providers of ICT products and services, and members of the cybersecurity research community and governments who find vulnerabilities has been proven to significantly increase both the rate of discovery and the remedy of vulnerabilities. Coordinated vulnerability disclosure specifies a structured process of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. The process also provides for coordination between the finder and the organisation as regards the publication of those vulnerabilities.

Some Member States have put in place coordinated vulnerability disclosure policies that further facilitate the cooperation of all involved stakeholders.

Q1: How do you evaluate the level of effectiveness of such national policies in making vulnerability information available in a more timely manner?

- ❑ Very low level
- ❑ Low level
- ❑ Medium level
- ❑ High level
- ❑ Very high level
- ❑ Don't know / no opinion

Q2: Have you implemented a coordinated vulnerability disclosure policy?

- ❑ Yes
- ❑ No
- ❑ Don't know / no opinion
- ✓ **Not applicable**

Q3: How would you describe your experience with vulnerability disclosure in the EU and how would you improve it?

1000 character(s) maximum

Vulnerability disclosure should be limited to government information sharing with the industry. Otherwise CSIRTs would be inundated with information e.g. the reporting of thousands of patch misconfigurations is not helpful. Further, consideration should be given to how existing mechanisms (including through CSIRTs) could be better leveraged and aligned with the

regulatory reporting regimes. In any case, separating regulatory functions from CSIRTs – which is not the case in all Member States – is paramount.

Q4: Should national authorities such as CSIRTs take proactive measures to discover vulnerabilities in ICT products and services provided by private companies?

1000 character(s) maximum

Sub-section 3.d. – Security of connected products

The constantly growing proliferation of connected products creates enormous opportunities for businesses and citizens but it is not without its challenges: a security incident affecting one ICT product can affect the whole system leading to severe impacts in terms of disruption to economic and social activities.

Q1: Do you believe that there is a need of having common EU cybersecurity rules for connected products placed on the internal market?

- ❑ Yes
- ✓ **No**
- ❑ Don't know / no opinion

Sub-section 3.e. – Measures to support small and medium-sized enterprises and raise awareness

A few Member States have taken measures to raise the levels of awareness and understanding of cyber risk amongst small and medium-sized enterprises. Some Member States are also supporting such companies in dealing with cyber risk (for example by disseminating warnings and alerts or by offering training and financial support).

Q1: To what extent do you agree with the following statements regarding such measures?

	Strongly disagree	Disagree	Agree	Strongly disagree	Don't know / no opinion

Such measures have proven to be effective in increasing the level of awareness and protection amongst SMEs.					
European legislation should require Member States to put in place frameworks to raise awareness amongst SMEs and support them.					