FESE response to the Commission consultation on the revision of the NIS Directive

2nd October 2020

***Can you specify further your capacity in which you are replying to the questionnaire on the review of the NIS Directive?**

X Trade association representing both entities currently covered and entities not covered by the NIS Directive

Please specify the sector you are responsible for:

Regulated markets

***Before starting this survey, are you aware of the objectives and principles of the EU Directive on security of network and information systems (the NIS Directive)?**

These comprehend:

- Member States' preparedness by requiring them to be appropriately equipped
- Cooperation among all the Member States, by setting up a cooperation group
- Set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks
- A culture of security across sectors
- OES to take appropriate security measures and to notify serious incidents to the relevant national authority
- DSP to comply with the security and notification requirements under the Directive.

☒Aware

***Has your organisation been impacted by the adoption of the NIS Directive (for example by having to adopt certain measures stemming directly from the Directive or from national laws transposing the Directive, or by participating in the various cooperation fora established by the Directive)?**

☒Yes

☐No

☐Don't know / no opinion

1. Section 1: General questions on the NIS Directive

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

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)?**

☒Don't know / no opinion

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

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

FESE considers that all technological advances currently under research or implementation should be part of the scope (e.g. quantum tech, cloud tech, AI, behaviour analysis, etc.).

FESE favours the harmonisation of the already existing rules on cybersecurity at EU level. We believe that actors in the financial sector, including highly regulated ones, should be able to use new technologies without unproportionate burden. Proportional standardised requirements across the financial sector would improve the overall resilience (e.g. in the cloud sector, we would propose the use of minimum standard requirements to facilitate its use and to avoid fragmentation). Nevertheless, where NCAs can supervise, this should be encouraged due to their knowledge of local markets.

On a general note, size is not the most relevant metric when determining what cybersecurity requirements should apply. Rather, entities should be subject to similar requirements if they show similar risk profiles and activities.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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

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					
Manufacturing					
Chemicals					
Wastewater					
Social networks			X		
Data centres				X	

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q2 - Should undertakings providing public communications networks or publicly 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

If yes, please elaborate your answer:

FESE believes this would allow a uniform approach in incident responses across the EU.

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

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:

The focus of the review should be to harmonise the existing diverging frameworks at EU / Member States level and to avoid further fragmentation. Nevertheless, we believe that the scope of the Directive should be extended beyond financial institutions.

While we believe that Member States specific expertise should be acknowledged, we would favour the adoption of a Regulation rather than a Directive as this allows for a clear rule-set.

Sub-section 1.g. - Information sharing

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

2. Section 2: Functioning of the NIS Directive

Sub-section 2.a. – National strategies

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

If yes, please specify which elements:

Certification in the EU, following also international cybersecurity standards, should become a possibility in order to comply with EU cybersecurity rules. With this provision, it would become easier to review new contract parties. Nevertheless, this option should remain not compulsory.

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

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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 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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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			X			
Cooperation with the Cooperation Group			X			
Cooperation with the CSIRTs network			X			

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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:

We believe a higher level of cooperation between Member States will increase the efficiency and efficacy of the overall ecosystem resilience against cyberattacks. In particular, FESE supports a higher level of harmonisation in defining the rules on how to identify OES at EU level. We sustain the idea that a harmonised identification process would contribute to a level playing field for companies from the same sector across Member States, although we do not know the details of this process in practice.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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 answers:

We believe more participants in the financial sector could potentially have a high impact in the overall processes. The current scope of the NIS Directive is quite limited.

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?

We believe that, if a function in a sector is in the scope of the NIS Directive, then all companies offering the same function should adhere to the same rules, according to the principle of "same business, same risk, same rules".

Additional sectors that should be covered by the scope of the NIS Directive are Cloud service providers, Internet service provider, and other providers on the digital infrastructure of services.

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
Financial market infrastructures				X		

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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
Financial market infrastructures					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)?

N/A

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?

N/A

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

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

N/A

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 ?

N/A

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)?

N/A

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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 explanation:

Cloud computing services - Currently, as the regulatory landscape is very fragmented, it is not possible to make an assessment for the whole EU. The scope of the different sector-specific regulatory frameworks seems to differ and this has proven to be problematic, as several companies from different sectors are using equivalent cloud computing services. Therefore, FESE believes that the scope of the Directive should be extended beyond its current reach as the financial sector is highly interconnected with a wide range of different companies (e.g. cloud computing services providers should be included as well).

Online marketplaces – N/A,

Online search engines – N/A

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						
Online search engines						
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?

N/A

Sub-section 2.e. - Security requirements

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Please elaborate your answer:

According to an internal FESE membership survey on cybersecurity topics, we found that Exchanges designated as OES reported increased security requirements as well as enhanced reporting obligations, with an overall increase in security practices. FESE Members are mostly positive about OES designations, alongside enhanced collaboration with security forces and supervisors.

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

N/A

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**

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

If yes, please specify for which sectors and elaborate:

Yes, we see sectoral differences, especially as security requirements are already partly integrated in sectoral legislation (e.g. EMIR, MiFID II/MiFIR, CCP Recovery and Resolution regime). In our view, the OES should have the liberty to assess and define the state of the art of the technology and the associated risks, allowing for flexibility to act properly. We would recommend a collaboration between the industry and national competent authorities to define such technology state of the art.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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 ensure a higher level of cybersecurity than general risk management obligations.					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 answers:

We are unsure of the meaning of 'prescriptive' in practice. In general, FESE would caution against overly prescriptive measures which would rapidly be outdated due to technological evolution. Instead, we would advocate for solutions that ensure the necessary flexibility.

Any requirement to disclose details on cyber resilience should be conducted carefully. Members States' requirements should be sufficiently comprehensive to encompass multiple cyber risks, avoid recommending technology-specific parameters. Alignment with global certifications would be beneficial.

Nevertheless, compliance with some sectoral requirements can be challenging, as these are formulated in an excessively broad language, especially where more EU regulatory authorities are involved. More detailed but not technology-prescriptive requirements would be helpful from an operational perspective. Supervisory convergence would benefit from more targeted detailed requirements and create a clear baseline framework.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Sub-section 2.f. – Incident notification

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 answers:

FESE Members experienced different approaches in incidents reporting requirements. We believe this is an unnecessary impediment to reaching the goal of keeping the sector resilient. A typical multijurisdictional company in the EU will likely have an incident response team operating across borders in a harmonised fashion. Although, an incident (impacting multiple locations) must be reported to different entities, via different formats, with different deadlines. This process is time consuming and takes attention away from the critical situation at hand. We strongly support a harmonised reporting process to local authorities which improves efficiency and aims at swiftly addressing critical incidents.

Nevertheless, this issue is residual for market participants active in a single jurisdiction. Any legislative proposal should carefully consider the possible market impact, taking also into account the differences between Trading Venues. Disproportional regulatory approaches should be avoided.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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 on the level playing field for companies in the internal market.				X	
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 answers:

FESE agrees with the statements above. We believe that a higher level of cooperation between Member States will increase the efficiency and efficacy of the overall ecosystem resilience against cyberattacks. In particular, FESE supports a higher level of harmonisation at EU level of the existing cybersecurity rules.

Sub-section 2.h. - Enforcement

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

There is a sufficient degree of alignment of penalty levels between the different Member States.					X

Sub-section 2.i. – Information exchange

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 agree	Don't know / no opinion
The Cooperation Group has been of significant help for the Member States to implement the NIS Directive.			x		
The Cooperation Group has played an important role in aligning national transposition measures.					X
The Cooperation Group has been instrumental in dealing with general cybersecurity matters.					X
The Cooperation Group is dealing with cross- border dependencies in an effective manner.					X
The CSIRTs network has effectively managed to fulfil its tasks as laid down in the NIS Directive.			X		
The CSIRTs network has helped to build confidence and trust amongst its members.			X		
The CSIRTs network has achieved swift and effective operational cooperation.					X
The Cooperation Group and the CSIRTs network cooperate effectively.					X

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

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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:

According to an internal FESE survey, we found a significant correlation between being an OES and being designated as a critical infrastructure. In fact, more than 50% of Exchanges being designated as national critical infrastructures are also in scope of the NIS Directive. FESE Members are mostly positive towards the designation in these two categories.

As noted above, FESE believes that compliance the NIS Directive and other sectoral legislation such as MiFID II/R, CSDR and GDPR have increased cyber resilience measures across the financial sector. However, the inclusion of digital and/or cyber resilience in most recent legislative measures have led to a cumulation of requirements, many of them being quite high level. Harmonisation of the existing diverging frameworks at EU and member states levels ought to be in focus.

Please also refer to our answer in Q2, sub-section 2.j.

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

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

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

FESE believes that increasing the level of expertise and number of experts at governments would lead to further willingness to share and discuss. Governments would need to show their added value in facilitating the sharing of information. Confidentiality and the ability to share information without any further regulatory consequences (with the aim to share and prevent future attacks) is key.

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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.)?

N/A

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

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
Financial market infrastructures			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?

FESE believes that increasing the level of expertise and number of experts at governments would lead to further willingness to share and discuss with the government as a facilitator. Governments would need to show their added value in facilitating the sharing of information. Confidentiality and the ability to share information without any further regulatory consequences (with the aim to share and prevent future attacks) is key.

Finally, since exchanging intel would be more valuable with additional detailed information, we would also propose a platform operated by an EU/Member State authority with anonymous membership. In that way companies could share their insights without the fear of repercussion.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

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? N/A

Q3 - How would you describe your experience with vulnerability disclosure in the EU and how would you improve it? N/A

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

Yes.

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

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

If yes, please elaborate your answer

FESE believes there is a need to have common EU cybersecurity rules for connected products placed on the internal market. If connected products are offered, while only some of them are aligned with the EU cybersecurity standards, there would be limited impact on connected products overall. The part of the connected products not subject to the EU framework would expose the other part (the resilient part) to possible risks.

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

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

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80