Public consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures

Fields marked with * are mandatory.

Public consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures

Purpose

On 6 May 2015, the European Commission adopted the Digital Single Market (DSM) Strategy, which provides for establishing a contractual Public-Private Partnership (cPPP) on cybersecurity in the area of technologies and solutions for online network security in the first half of 2016.

The Commission is now consulting stakeholders on the areas of work of the future cybersecurity contractual public-private partnership. The Commission is also calling for contributions on potential additional policy measures that could stimulate the European cybersecurity industry.

With respect to cybersecurity standardisation, this consultation complements the overall public consultation on the development of the Priority ICT Standards Plan: "Standards in the Digital Single Market: setting priorities and ensuring delivery", in which cybersecurity is one of the areas covered.

The Commission will use the feedback from the consultation to establish the cPPP in the first half of 2016.

Background

Current EU policies, such as the Cybersecurity Strategy for the European Union and the Commission's proposal for a Directive on Network and Information Security, aim to ensure that network and information systems, including critical infrastructures, are properly protected and secure.

A lot of work has already been done with industrial stakeholders within the NIS Platform. In particular the NIS Platform Working Group 3 has finalised a Strategic Research Agenda for cybersecurity which serves as the basis for the questions on prioritising research and innovation topics in this consultation.

The establishment of a contractual Public-Private Partnership addressing digital security would be a further step towards cybersecurity industrial policy. The Commission is now considering what additional industrial measures may be needed to complement the cPPP.

The cPPP will be a contractual arrangement between the Commission and an industrial grouping, both of which are committed to supporting, in the EU's Horizon 2020 programme, research and innovation activities of strategic importance to the Union’s competitiveness in the field of cybersecurity.

A contractual PPP bringing together industrial and public resources would focus on innovation following a jointly-agreed strategic research and innovation roadmap. It would make the best possible use of available funds through better coordination with member states and a narrower focus on a small number of technical priorities. It should leverage funding from Horizon 2020 to deliver both technological innovation and societal benefits for users of technologies (citizens, SMEs, critical infrastructure), as well as provide visibility to European R&I excellence in cyber security and digital privacy. Furthermore cybersecurity is explicitly identified in the DSM strategy as a priority area in which there is a need to define missing technological standards.

Duration

Opens on 18 December 2015 – closes on 11 March 2016 (12 weeks)

Comments received after the closing date will not be considered.

Who should respond

- Businesses (providers and users of cybersecurity products and services);
- Industrial associations
- Civil society organisations
- Public authorities
- Research and academia
- Citizens

Transparency

Please state whether you are responding as an individual or representing the views of an organisation. We ask responding organisations to register in the Transparency Register. We publish the submissions of non-registered organisations separately from those of registered ones as the input of individuals.

How to respond

Respond online

You may pause any time and continue later. You can download a copy of your contribution once you've sent it.

Only responses received through the online questionnaire will be taken into account and included in the report summarising the responses, exception being made for the visually impaired.

Accessibility for the visually impaired

We shall accept questionnaires by email or post in paper format from the visually impaired and their representative organisations: download the questionnaire

Email us and attach your reply as Word, PDF or ODF document

Or

Write to

European Commission

DG Communication networks, content & technology

Unit H4 – Trust & Security
25 Avenue Beaulieu
Brussels 1049 - Belgium

Replies & feedback

We shall publish an analysis of the results of the consultation on this page 1 month after the consultation closes.

Protection of personal data

For transparency purposes, all the responses to the present consultation will be made public.

Please read the Specific privacy statement below on how we deal with your personal data and contribution.

- Protection of personal data
- Specific privacy statement

References

Current EU policies in the field:

- Cybersecurity Strategy for the EU
- EC proposal for a Directive on Network and Information Security
  - Work on online privacy
  - Work with stakeholders in the Network and Information Security Platform

Contact

CNECT-FEEDBACK-CYBERSECURITY-DSM@ec.europa.eu

General information on respondents

Please note that fields marked with * are mandatory.

* Do you wish your contribution to be published?

Please indicate clearly if you do not wish your contribution to be published

- (•) Yes
- ( ) No

Submissions that are sent anonymously will neither be published nor taken into account.

*

The Commission may contact you in case a clarification regarding your submission is needed depending on your reply to the following question.

Do you wish to be contacted?

- (•) Yes
- ( ) No

* I'm responding as:

- ( ) An individual in my personal capacity
- (•) The representative of an organisation/company/institution

Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

- (•) Yes
- ( ) No

Please give your organisation's registration number in the Transparency Register. We encourage you to register in the Transparency Register before completing this questionnaire. If your organisation/institution responds without being registered, the Commission will consider its input as that of an individual and publish it under that heading.

08957111909-85

Please tick the box that applies to your organisation and sector.

- ( ) National administration
- ( ) National regulator
- ( ) Regional authority
- ( ) Non-governmental organisation
- ( ) Small or medium-sized business
- ( ) Micro-business
- (•) European-level representative platform or association
- ( ) National representative association
- ( ) Research body/academia
- ( ) Press
- ( ) Other

My institution/organisation/business operates in:

- [x] All EU member states
- [ ] Austria
- [ ] Belgium
- [ ] Bulgaria
- [ ] Czech Republic
- [ ] Croatia

- [ ] Cyprus
- [ ] Denmark
- [ ] Estonia
- [ ] France
- [ ] Finland
- [ ] Germany
- [ ] Greece
- [ ] Hungary
- [ ] Italy
- [ ] Ireland
- [ ] Latvia
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta
- [ ] Netherlands
- [ ] Poland
- [ ] Portugal
- [ ] Romania
- [ ] Spain
- [ ] Slovenia
- [ ] Slovakia
- [ ] Sweden
- [ ] United Kingdom
- [x] Other

* Please enter the name of your institution/organisation/business.

ETNO - European Telecommunications Network Operators' Association

* Please enter your name

Marta Capelo

* Please enter the address of your institution/organisation/business

Boulevard du Regent 43-44 Brussels, 1000

* What is your place of main establishment or the place of main establishment of the entity you represent (headquarters)?

Belgium

Consultation

Note:

- *Depending on the question please make either one choice or multiple choices in responses to specific questions*
- *Please note that a character limit has been set for most open questions*

I. Identification of your priorities in cybersecurity

* 1. Which part of the value chain of cybersecurity services and products do you represent?

- [ ] Researcher
- [x] Customer/User
- [x] Supplier of cybersecurity products and/or services
- [ ] Public authority/government agency responsible for cybersecurity/research

If you answered "customer/user", which specifically?

- [ ] Certification/audit or standardisation agent
- [ ] Individual user
- [ ] SME user
- [x] Private enterprise
- [ ] Public user
- [ ] Civil Society
- [ ] Other

2. Which of the following describes the cybersecurity activities of your institution/organisation/business? (multiple answers possible)

2.1. Dedicated Cybersecurity -> Cybersecurity products/services

- [x] Identity and access management
- [x] Data security
- [x] Applications security
- [x] Infrastructure (network) security
- [x] Hardware (device) security
- [x] IT security audit, planning and advisory services
- [x] IT security training
- [ ] Other

If you answered "other", please specify

400 character(s) maximum

2.2. Applied Cybersecurity -> Application areas with demand in cybersecurity products/services

- [x] Critical infrastructures in general

- [ ] Energy
- [ ] Transport
- [ ] Health
- [x] Finance and Banking
- [x] Public Administration
- [ ] Smart Cities
- [x] Digital Service Providers
- [x] Protection of individual users
- [x] Protection of SMEs
- [ ] Other

Please specify:

400 character(s) maximum

Because telecom networks are the physical foundation of all digital networks (public and private, Internet, VPN, etc.) and services, there are specific cybersecurity issues at the level of connectivity and network (e.g. virtualization).
These are not necessarily addressed by on the shelf products and services addressing private network security.

2.3. Applied Cybersecurity -> Specific IT technology areas with cybersecurity as a functional requirement

- [x] Internet of Things
- [ ] Embedded Systems
- [x] Cloud Computing
- [x] 5G
- [x] Big Data
- [x] Smartphones
- [x] Software Engineering
- [x] Hardware Engineering
- [ ] Other

Please specify:

400 character(s) maximum

Evolution of communication technologies raise new cybersecurity issues: examples include 5G but also issues such as network virtualization.

II. Assessment of cybersecurity risks and threats

1. Risk identification

*

1.1. What are the most pressing cybersecurity challenges for users (individuals, business, public sector)?

between 1 and 3 choices

- [x] Loss of know-how and confidential business information (trade secrets) – industrial and economic espionage, and other types of confidential information
- [x] Industrial or economic sabotage (examples: disrupting or slowing down network and computer functioning)
- [x] Extraction and use of identity and payment data to commit fraud
- [ ] Intrusion in privacy
- [ ] Other

* Please specify:

1200 character(s) maximum

_

* 1.2. Which sectors/areas are the most at risk? (please choose top 3-5)

between 3 and 5 choices

- [x] Critical infrastructures in general
- [ ] Energy
- [ ] Transport
- [ ] Health
- [x] Finance and Banking
- [x] Public Administration
- [ ] Smart Cities
- [x] Digital Service Providers
- [x] Protection of individual users
- [ ] Protection of SMEs
- [ ] Other
- [ ] I don't know

Please specify:

400 character(s) maximum

2. Preparedness

* 2.1. Are the necessary products/services available on the European market to ensure security of the whole value chain

- ( ) Yes
- (•) No
- ( ) I don't know

If no, which are missing - please provide examples:

400 character(s) maximum

In general, the market lacks cybersecurity products made in the EU. Moreover, there are other topics for which the global market lacks cybersecurity products: this is the case for securisation of virtualized networks, but also more use of big data techniques in the field of cybersecurity. Even where there are products that are adequate for today's challenges, they will soon be out of date.

2.2. If relevant, where do the cybersecurity products/services you purchase come from?

- [x] National/domestic supplier
- [x] European, non-domestic supplier
- [x] US
- [x] Israel
- [x] Russia
- [x] China
- [ ] Japan
- [ ] South Korea
- [x] Other

If you answered "other", please specify

200 character(s) maximum

Issues are not only about cybersecurity products but also about implementation of cybersecurity features in regular products: these regular products can be purchased from all types of vendors too.

2.3. If relevant, what are the reasons behind your decision to choose non-European ICT security products/services over European ones?

- [x] Price competitiveness
- [x] Non-European products/services are more innovative
- [x] Trustworthiness
- [ ] Interoperability of products/solutions
- [x] Lack of European supply
- [ ] Place of origin is irrelevant
- [x] Other

If you answered "other", please specify:

800 character(s) maximum

Brand image - Very often companies trust in security solutions provided by well-known foreign firms.
Integration - Often companies prefer built-in security solutions of the traditional vendors (i.e. groupware, identity management, network management…)

rather than to add third party security layers over this, even though the native security features are potentially poor.

2.4. If relevant, what are the reasons for missing supplies of products/services in cybersecurity?

- [x] Lack of capital for new products/services
- [x] Lack of sufficient (national/European/global) demand to justify investment
- [x] Lack of economics of scale for the envisaged (national/European/global) markets
- [x] Market barriers
- [ ] Other
- [ ] I don't know

If in question 2.4. you marked "Market barriers", please specify:

- [ ] In the EU member state you operate
- [x] Between EU member states
- [x] Globally
- [x] Between industry sectors
- [ ] Other

3. Impact

* 3.1. In which of the following areas would you expect the worst potential socio-economic damage? (please choose your top 1-5 answers)

between 1 and 5 choices

- [x] Critical infrastructures
- [ ] Energy
- [ ] Transport
- [ ] Health
- [x] Finance and Banking
- [x] Public Administration
- [ ] Smart Cities
- [x] Digital Service Providers
- [ ] Protection of individual users
- [x] Protection of enterprises (large companies and/or SMEs)
- [ ] Other
- [ ] I don't know

Please specify/explain

1200 character(s) maximum

4. Cybersecurity challenges by 2020

4.1. What will be the 3 main cybersecurity challenges by 2020? (Please explain)

1200 character(s) maximum

In general terms, the main Cybersecurity challenges can be aligned in three main areas:
- Keeping pace with evolving and escalating threats (i.e. from IoT applications)
- Coping with changing technology and business practices (innovating securely, network protection specially in 5G networks)
- Achieving a balance between the rights of individuals and collective security (plus the burden on industry on implementing the solution)

III. Cybersecurity Market Conditions

1. To what extent are markets in cybersecurity products/services competitive in Europe? Please provide your assessment of the overall situation in Europe and your views on the particular sectors of your expertise

1200 character(s) maximum

- supply is limited in the EU, very dependent from 3rd country-based providers
- users' selection criteria can still be linked to brand names or nationality of providers
- this might be due to the lack of European trust labels that can apply to products but also to companies
- non-uniform Member States legislations and lack of a real single market making commercialization expensive and difficult
- lack of interoperability/standardised APIs/reference architectures means that integrated solutions from single providers are preferred to ad hoc best of breed solutions. This makes it hard for new entrants to break into the marker and for smaller players to compete even if they have a better point solution.

2. If you are a company headquartered in the European Union, how would you assess the situation of innovative SMEs and start-ups working in the field of cybersecurity and privacy in the European Union?
a. Please assess the ease of access to markets in EU countries other than your own
b. Please assess the opportunities for operating in the European Single Market

1200 character(s) maximum

EU based SMEs and start-ups face a difficult situation. SMEs also need to form ecosystems with larger players, which are very dependent on 3rd country-based suppliers and prefer to trust in well-established brands.

Harmonised rules across EU would:
- facilitate the development and marketing of cybersecurity products and features and
- promote access to the single market

Overall, a single European market could allow for an increase of the EU firms' average size enabling them to withstand competition from outside the EU.

3. If you are a company headquartered outside the European Union, please
a. assess the ease of accessing the EU market
b. assess the opportunities for operating in the European Single Market
c. explain how much you have invested or intend to invest in Europe over the past/next five years respectively?

1200 character(s) maximum

4. How does European competitiveness compare to other countries/regions? In particular what are the strengths and weaknesses of European cybersecurity solution providers (self-assessment if you are a supplier)?

1200 character(s) maximum

Strengths:
- High skilled professionals, good knowledge, situation awareness, good image among emergent markets, good level of security of the traditional service providers (eg.: telco sector).

Weaknesses:
- Fragmentation, small size, lack of brand image, adverse regulatory environment, brain drain.

5. Which level of ambition do you think the EU should set itself for cybersecurity market development? (Please mark for each category.)

	Retain global lead	Strive for global leadership	Make EU more competitive
*Identity and access management	○	◉	○
*Data security	○	◉	○
*Applications security	○	○	◉
*Infrastructure (network) security	◉	○	○
*Hardware (device) security	○	○	◉
*IT security audit, planning and advisory services	○	○	◉

*IT security management and operation services	○	◉	○
*IT security training	○	○	◉

6. How does legislation (currently in force or soon to be adopted) influence the European cybersecurity market(s) or how is it likely to do so?

1200 character(s) maximum

Although the rate of change in Cybersecurity is much more rapid than the ability of legislation to keep up, legislative measures are an important step in the good direction. The NIS Directive is a good example. Indeed, legislation can influence the market in the same way that other safety regulations influenced other markets in the past (eg.: car safety, aeronautics and aviation, etc.). However, in order to achieve a level playing field, regulation in cybersecurity should cover not only those companies based in EU, but any service provider offering services to the EU.

Additionally, privacy regulation applied to cybersecurity is strongly fragmented and protective, hampering the collaboration in markets and products. Nevertheless, we positively asses the General Data Protection Regulation, which precisely aims to be applicable to all businesses providing services to EU residents.

7. How does public procurement impact the European cybersecurity market? :

- ◉ It is a driver behind cybersecurity market development and an opportunity for companies to increase market share,
- ○ It is a barrier to market access
- ○ I don't know

Please explain

1200 character(s) maximum

Public procurement should be the driver of a future cybersecurity industry in Europe with focus on a product driven innovation. Public procurement can help to make a provider or a vendor credible.

However, reality shows that currently public procurement can be a clear barrier due to the fragmentation based on domestic consumption of products and services and an implicit preference for national choices.

8. Do you feel you have sufficient access to financial resources to finance cybersecurity projects/initiatives?

- ○ Yes
- ◉ No

9. What are the types of financial resources you currently use?

- [ ] Bank loans
- [ ] Equity funds
- [x] Venture funds
- [ ] EIB/EIF support
- [ ] Sovereign welfare funds
- [ ] Crowd funding
- [ ] EU funds
- [x] Other

If "other", please specify:

600 character(s) maximum

Generally speaking, ETNO companies use own funds to finance cybersecurity projects and initiatives.

10. Do you feel that the European ICT security and supply industry has enough skilled human resources at its disposal?

- ( ) Yes
- (•) No
- ( ) I don't know

Please explain

1200 character(s) maximum

Every company competes for the same profiles.

11. Have you ever experienced any barriers related to market access and export within the EU and/or beyond EU countries?

- (•) Yes
- ( ) No

Please describe

1200 character(s) maximum

Even if not formal barriers, nationality of “vendors” can play a role. Furthermore, the fragmentation of the EU market imposes a de facto barrier for the deployment of cybersecurity products across the EU.

12. Are you aware of any start-up policy measures for cybersecurity industry in your country/the European Union?

- (•) Yes
- ( ) No

Please describe:

1200 character(s) maximum

There are several public and private initiatives to promote the launching of companies and the capture of talent, such as:

Spain
- Public Sector – Important role played by INCIBE (Spanish Institute for Cybersecurity)
- Private Sector – BBVA Bank, Telefónica have developed specific cybersecurity programs (eg.: “National Antibotnet Protocol”)

UK
- Public Sector: UK Government https://www.gov.uk/government/news/making-cyberspace-cyber-safe-new-government-initiative-for-cyber-startups-will-drive-innovation
- Private Sector – BT Innovation

Italy
- Public Sector: Important role played from the National CyberSecurity Laboratory CINI (national Interuniversity Consortium for Informatics)
- Private Sector: TIM invested in 2015 in start-up companies specialized in cybersecurity

IV. Need for public intervention and support for a functioning market in cybersecurity products/services in Europe

1. In your opinion, in what areas does the European market for cybersecurity products and services function well and where would public intervention be unnecessary or even detrimental? (Please specify)

1200 character(s) maximum

The areas where the European market for cybersecurity products and services function better are those related with human capital and user awareness
- Other areas require major improvements, inter alia: (1) regulation, (2) program endorsement, (3) financing, (4) R&D or (5) standardization.
- It is expected that public intervention would play an important role.

2. What problems need to be addressed at European level to achieve a functioning Digital Single Market in cybersecurity products/services? (Please specify)

1200 character(s) maximum

Areas where major improvements are required:
- regulation
- programme endorsement
- financing

- R&D
- Standardization
- Interoperability of security solutions(i.e. fostering open standards, open API ecosystems and open architectures)

3. How do you assess public support and intervention at national level with regard to the cybersecurity market? How useful / necessary / adequate is it? (Please specify)

1200 character(s) maximum

Any support of skills at national level is necessary and useful.

4. Please provide examples of successful support through public policies (at national or international level).

1200 character(s) maximum

-

V. Specific Industrial Measures

The first question in this section complements the overall public consultation on the Priority ICT Standards Plan with respect to the specific characteristics of cybersecurity standardisation. We understand by standardisation in this context the production of technical specifications, standards or architectures where there is a need/gap, but also any other type of standardisation action such as landscape analysis, gap finding, roadmaps or ecosystem building.

1. How would you evaluate the current role of standardisation in the domain of cybersecurity?

* 1.1. Have you applied or are you currently working with specific technical specifications, standards or architectures relevant to cybersecurity?

1200 character(s) maximum

Yes. Many ETNO companies are currently involved in international standardisation bodies like ETSI, ITU, GSMA, ISO, 3GPP, Cloud Security Alliance, NIST/FIPS, Federal Office for Information Security (BSI), DAWSP, PCI/DSS.

1.2. In what areas is there a need/gap in this respect?

1200 character(s) maximum

- assessment side
- extend common criteria
- coordination side

*

1.3. Would you consider standardisation as a mean to support innovation and the digital single market in cybersecurity?

- (•) Yes
- ( ) No
- ( ) I don't know

* Please explain your view

1200 character(s) maximum

- In a sense there are too many standards. Attempts have been made to map / inter relate these but this in itself creates confusion.
- Standardization is a precondition for the new incomers to compete with incumbents, manufacturers and digital service providers, in the field of cybersecurity.
- Standardisation is an outreach of research activity. It allows to expose innovation results and that stakeholders adopt best technical and procedure solutions.
- However, the strong influence of industry big players when they impose “de facto” standards tailored to specific products or services distorts the standardization goals.
- In a way, there are too many standards. Attempts have been made to map/inter relate these but this in itself creates confusion.
- On top of that, the extremely long standardisation timings are not aligned with real innovation. There is also the danger that out of date, poorly written or inappropriate standards can hamper innovation, impose unnecessary burdens and divert effort from where it is needed.

* 1.4. Should standardisation in cybersecurity be addressed generically or should it focus on specific sectors (e.g. transport, energy, finance) and areas of application (e.g. connected vehicles, smart-grids, electronic payments)? (Please specify your choice)

1200 character(s) maximum

In principle, standardisation in cybersecurity should be addressed generically.
When it comes to specific focus, it would be more effective to approach it by specific areas of applications (rather than by specific sectors), addressing specific needs and constraints of specialized vertical security solutions. It could also segment by criticality of requirements in the various features of security (confidentiality, integrity, availability).

* 1.5. What areas should future cybersecurity standardisation efforts focus on? (Please specify).

1200 character(s) maximum

- IoT, Industrial security
- Cryptography
- Metrics and measurements
- Information exchange, data sharing of threat intelligence

- Privacy
- Interoperability

2. Assessment of existing certification schemes in the field of cybersecurity

* 2.1. Are you active in public or private certification bodies?

- (•) Yes
- ( ) No

* If yes, please specify:

600 character(s) maximum

Some ETNO companies are active in public and private certification bodies

2.2. Which existing ICT security certification schemes would you consider successful and what learnings should be taken from them for future cybersecurity certification activities?

1200 character(s) maximum

- Common criteria
- Security techniques: Information security management systems – Requirements ISO 27001
- Payment Card Industry Data Security Standard PCI DSS
- Federal Information Processing Standard – Security Requirements for Cryptographic Modules – FIPS

* 2.3. Do the current ICT security certification schemes adequately support the needs of European industry (either supplying or buying cybersecurity solutions)?

- ( ) Yes
- (•) No
- ( ) I don't know

Please explain

1200 character(s) maximum

- Current security certification schemes do not have scale. They will drive the EU to a blockage if each stakeholder distrust to each other.
- Security certification schemes are very expensive and time consuming processes and there are now too many different certifications at world level. The EU should address this situation urgently.
- An acceleration in the process to publish these certification schemes would be appreciated.

* 2.4. How relevant are certification schemes to the digital single market in cybersecurity products and services?

1200 character(s) maximum

Certification schemes are essential to the digital single market to build trust within the single market.

* 2.5. What areas should future certification efforts focus on?

1200 character(s) maximum

- industrial and IoT Security
- Cybersecurity services and products
- Professional services

* 2.6. Are certification schemes mutually recognised widely across European Union's Member States?

- (•) Yes
- ( ) No
- ( ) I don't know

* Please specify

1200 character(s) maximum

It depends. But sometimes, there is no mutual recognition

* 2.7. Is it easy to demonstrate equivalence between standards, certification schemes, and labels?

- ( ) Yes
- (•) No
- ( ) I don't know

Please explain

1200 character(s) maximum

The inclusion of trusted third parties involved in:
- The Assessment of compliance with standards or other reference
- The mapping of various certifications and labels

would facilitate the equivalence between standards, certification schemes and labels.

However, in general, certification is very time consuming and costly. A convergence of certifications would certainly help users (better understanding) and providers.

* 3. Are you aware of any existing labelling schemes for cybersecurity products and services in Europe or in the rest of the world?

- (•) Yes
- ( ) No

* 3.1. If yes, please specify if you are referring to legal labelling schemes or industry self-labelling schemes.

600 character(s) maximum

ETNO companies consider that self labelling schemes do not provide any value for users/customers/buyers.

3.2. If yes, how do you assess the efficiency of such labels to provide visibility and readability for buyers?

800 character(s) maximum

* 3.3. How would you assess the need to develop new or expand existing labels in Europe?

1200 character(s) maximum

As there are already many certification schemes, the issue would not be about creating new labels but to expand approaches and ensure some convergence.

* 3.4. Which market(s) would most benefit from cybersecurity labels?

- [x] Consumer market
- [x] Professional market (SMEs)
- [x] Professional market (large companies)
- [ ] I don't know

3.5. What criteria / specific requirements are necessary to make such labels trustworthy?

1200 character(s) maximum

- Current labelling schemes have visibility, but they lack efficiency and readability.
- It would be urgent to extend labelling schemes to include new challenges and ensure convergence.
- Additionally endorsement of labels and use by Public Administration as early adopter would be an important element for further success.

* 4. What form of access to finance would be most useful for European cybersecurity industry players to encourage business growth?

between 1 and 5 choices

- [ ] Bank loans
- [ ] Equity funds
- [x] Venture funds
- [x] EIB/EIF support
- [ ] Sovereign welfare funds
- [x] Crowdfunding
- [x] EU funds, please specify

☐ Other

* Please explain

1200 character(s) maximum

Research Programmes and PPPs

5. What specific start-up policy measures do you consider useful for the cybersecurity industry in the European Union?

1200 character(s) maximum

Start-ups should be helped to scale-up without having to go to trade exit by for instance endorsement programmes by which in equal conditions, start-ups products should be purchased.

6. What do you think would be the right measures to support the EU market access and export strategy for cybersecurity products and services?

1200 character(s) maximum

- Policies to foster consumption of products and services manufactured by EU companies
- To create and invest in cybersecurity brands
- To foster good price/good quality EU products
- Harmonised regulation across the EU and harmonization with wider global standards

7. How would you assess the role of national/regional cybersecurity clusters (or national/regional cybersecurity centres of excellence) and their effectiveness in fostering industrial policies in the field of cybersecurity?

1200 character(s) maximum

National/regional cybersecurity clusters or national/regional cybersecurity centres of excellence play an adequate role as starting point in fostering industrial policies in the field of cybersecurity, especially they have a positive effect on skills, growth, human development. More should be done to focus on development of skilled work force and wider security awareness. It is important however to avoid duplication of efforts amongst them by adequate coordination mechanisms.

8. Are there any other specific policy instruments you think would be useful to support the development of the European cybersecurity industry?

1200 character(s) maximum

VI. The role of research and innovation in cybersecurity

1. Have you participated in previous R&I efforts through European (FP7, CIP) programmes?

- (●) Yes
- ( ) No

* 1.1. If yes, what was your assessment of this participation and the key outcome for your organisation?

1200 character(s) maximum

-

* 1.2. What was the main impact of the topics and projects funded in cybersecurity?

1200 character(s) maximum

-

* 1.3. What were the key shortcomings of how cybersecurity was addressed in past R&I programmes?

1200 character(s) maximum

-

* 1.4. To what extent would a single focal area like a contractual PPP address these earlier weaknesses?

1200 character(s) maximum

-

* 1.5. What other measures could facilitate SME participation in such programmes?

1200 character(s) maximum

ETNO companies have participated in the past in previous Research and Innovation efforts through European programmes. The main benefits being

- Sharing expertise
- Accelerating time to market
- Collaborative research in standardization

2. On which levels would you focus public support for research & innovation measures (please identify in % - total should be equal to 100%)?

	% (specify 0-5-10-15-25-50-100)
Fundamental research	5%
Innovation activities	15%
Using research & innovation results to bring products and services to the market	15%
Development of national/regional cluster (or national/regional centres of excellence)	5%
Start-up support	5%
SME support	10%
Public Procurement of innovation or pre-commercial support of development and innovation	0%
Individual, large-scale "Flagship" initiatives	10%
Coordination of European innovation and research activities	10%
Definition of common requirements for cybersecurity products and services for specific application domains at European level (e.g. transport, energy…)	25%
Other (please specify)	
TOTAL (100%)	

3. In which areas would a prioritisation of European support actions be most effective? (Please identify your 3-5 top priorities)

* 3.1. In terms of research priorities following the terminology of the Strategic Research Agenda of the NIS Platform [1]

between 2 and 3 choices

- [ ] Individuals' Digital Rights and Capabilities (individual layer)
- [x] Resilient Digital Civilisation (collective layer)
- [x] Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)
- [x] Other

Please specify:

800 character(s) maximum

```
It is necessary to highlight that the gaps are not well identified in the
Strategic Research Agenda elaborated by the NIS Platform.
```

* 3.2. In terms of products and services

between 3 and 5 choices

- [ ] Identity and access management
- [x] Data security
- [x] Applications security
- [x] Infrastructure (network) security
- [x] Hardware (device) security
- [ ] IT security audit, planning and advisory services
- [x] IT security management and operation services
- [ ] IT security training
- [ ] Other

Please explain:

600 character(s) maximum

4. In which sectors would a prioritisation of European support actions be most effective? (Please identify top 3 to 5 and explain)

between 3 and 5 choices

- [x] Critical infrastructure in general
- [ ] Energy
- [ ] Transport
- [ ] Health
- [ ] Finance and Banking
- [ ] Digital Service Providers
- [x] Internet of Things

- [x] Cloud Computing
- [x] Public Administration
- [ ] Other

Please explain your choice:

1200 character(s) maximum

5. In your opinion which bodies merit particular attention? (Please explain for each category you select)

- [x] Universities and Research Institutes
- [x] SMEs
- [x] Start-ups
- [x] Enterprises with large market share in nation markets ("National Champions")
- [x] Enterprises with strong positions on global markets ("Global players")
- [ ] Other

Please explain:

1200 character(s) maximum

All stakeholders are tightly coupled. SMEs, start-ups, Universities, Research Institutions would require particular attention. The active involvement of other actors in the ecosystem is also very important in order to maximize expected outcomes.

6. What are the specific needs of innovative SMEs in cybersecurity to stimulate competitiveness? What specific type of public support would be most useful to such companies?

1200 character(s) maximum

For the SMEs to be competitive in cybersecurity, a number of factors are required:
- talent in cybersecurity – education programmes and research centres need to invest in this line
- Awareness raising – to consider cybersecurity as a strategic issue
- Public support to respond to the strategic nature of cybersecurity (eg: by public funds, endorsement programmes)

* 7. What would be your contribution to fostering innovation and competitiveness of cybersecurity in Europe?

- [x] Support in alignment of national and European research agendas
- [x] Support for SMEs
- [x] Co-funding of national or European activities
- [x] Providing infrastructures for experimenting and testing
- [x] Support with expertise in standardisation bodies

- [x] Contribute to certification schemes
- [ ] Other

Please explain

1200 character(s) maximum

VII. The NIS Platform

This section is a separate part of the consultation, not related to the cPPP and accompanying measures, but looking for interested stakeholders' views on the public-private network and information security Platform (NISP).

The NIS Platform, which was one of the actions under the EU Cybersecurity Strategy, was established in June 2013. Its aim was to identify good cybersecurity practices that organisations can implement in order to increase their resilience. These practices were expected to facilitate the future implementation of the NIS Directive, but are also relevant to a wide range of organisations not covered by the Directive.

The Platform gathered almost 600 stakeholders representing the business community, civil society, academia, researchers and member states. NIS Platform work has been divided into three sub-groups dealing with risk management; voluntary information exchange and incident coordination as well as secure ICT research and innovation. Over the course of two years the working groups have developed a number of deliverables, including the Strategic Research Agenda, which feeds into the process of creating the contractual Private Public Partnership on cybersecurity addressed in the previous sections of this consultation.

The Commission would like to take the opportunity to ask stakeholders, who participated in the efforts of the NIS Platform, about their views on Platform's work to date. The Commission would also like to have the views of all interested stakeholders on the future of the NIS Platform. It will take these views into consideration in the process of developing a new Work Programme for the NIS Platform following the expected adoption of the NIS Directive in early 2016.

1. NIS Platform format - what did you like about the structure and working methods of the NIS Platform and what would you suggest changing (if anything)?

1200 character(s) maximum

Question for stakeholders who took part in the NIS Platform's work

The NIS Platform was a good attempt to put together a large group of stakeholders to discuss issues of common interest. However, the large number of participants was also a shortcoming, as it was difficult to build on the necessary trust relationship.

Moreover, as the NIS platform recruited on a volunteering basis, its constituency does not fully reflect the needs of the market, especially from the demand side.

This bias should be taken into account and redressed in deliverables produced by the platform: this is particularly visible in the Strategic Research Agenda which underestimates market gaps in its gap analysis.

2. What possible future areas of work should the NIS Platform focus on following the adoption of the NIS Directive?

1200 character(s) maximum

Question for all stakeholders

After the adoption of the NIS Directive, the NIS Platform should focus on the development of guidelines for the implementation of the NIS Directive

The NIS Directive is a step forward the right direction, although its final version does not cover the entire value chain of the digital economy, as it had been initially proposed by the Commission. Furthermore, the implementation is based on the principle of minimum harmonization (Article.2). This could be positive when it encourages Member States to adopt a higher level of protection than envisaged by the Directive. Nonetheless, the fragmentation of the legal landscape in the field of cyber protection will continue to exist, maintaining the regulatory burdens and the complexities for pan-European operators.

3. What were your reasons for engaging/not engaging in the NIS Platform's work so far?

1200 character(s) maximum

Question for all stakeholders

The resources involved are time consuming and the outcomes expected from the NIS platform are not very clear.

4. What would be your motivation for engaging in the NIS Platform's work after the adoption of the NIS Directive, and what expectations would you have?

1200 character(s) maximum

Question for all stakeholders

Clarifying expectations from the NIS platforms in terms of deliverables but also of available leverage would help stakeholders.

VIII. Sharing your data and views

* Please upload additional data and information relevant to this survey.

2000 character(s) maximum

Please refer to the attached document for additional data.

Please upload your file

- **6fab405a-bbe6-46a5-b7ba-ed7314eec6e4/Additional Data ETNO.pdf**

[1] For further information, please consult the Strategic Research Agenda of the WG3 Network and Information Security (NIS) Platform - https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-ag

Contact

✉ CNECT-FEEDBACK-CYBERSECURITY-DSM@ec.europa.eu