Case Id: 2d29e1c4-4d0e-4add-94b5-7798fbde07be
Date: 10/03/2016 20:24:05

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.

2702114689-05

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:

□ 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
☑ Other

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

OpenForum Europe Ltd

*Please enter your name

Diana Cocoru

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

73 Hillside Road, Ashtead, Surrey KT21 1SD, UK

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

UK

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
□ Customer/User
□ Supplier of cybersecurity products and/or services
□ Public authority/government agency responsible for cybersecurity/research

If you answered "Researcher", please specify

400 character(s) maximum

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

2.1. Dedicated Cybersecurity -> Cybersecurity products/services

□ Identity and access management
□ Data security
□ Applications security
□ Infrastructure (network) security
□ Hardware (device) security
□ IT security audit, planning and advisory services
□ IT security training
☑ Other

If you answered "other", please specify

400 character(s) maximum

OFE closely monitors the EU and international policy and legal developments around cybersecurity and provides input from technical and legal experts.

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

☑ Critical infrastructures in general
□ Energy
□ Transport
□ Health

□ Finance and Banking
□ Public Administration
□ Smart Cities
☑ Digital Service Providers
☑ Protection of individual users
□ Protection of SMEs
□ Other

Please specify:

400 character(s) maximum

□

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

☑ Internet of Things
□ Embedded Systems
☑ Cloud Computing
□ 5G
☑ Big Data
□ Smartphones
□ Software Engineering
□ Hardware Engineering
□ Other

Please specify:

400 character(s) maximum

□

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

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

* Please specify:

1200 character(s) maximum

It is unclear what is meant by ‘intrusion in privacy’. We take the view that the term ‘privacy’ goes beyond personal privacy.

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

between 3 and 5 choices

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

Please specify:

400 character(s) maximum

‘Digital Service Providers’ is not an appropriate sector classification. Instead we believe the proper classification should be IT/telecommunications.

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

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

□ National/domestic supplier
□ European, non-domestic supplier
□ US
□ Israel
□ Russia
□ China

☐ Japan
☐ South Korea
☑ Other

If you answered "other", please specify

200 character(s) maximum

We question how one would categorize a ‘European/non-domestic supplier’? Does this strictly refer to the geographical location of a company’s development capabilitie, the hq or source of investment?

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

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

If you answered "other", please specify:

800 character(s) maximum

We believe the wrong question is being asked and this reflects a lack of understanding of the marketplace. When one closely looks at cybersecurity solutions, they typically go through EU distributors. Intermediaries or system integrators will collect a number of solutions and integrate them for their customer. Pure European players are successful in this sector. There is no differentiation between the manufacturer, sales, after sales, and distributor in the final solution.
Other dimensions worth drawing attention to:
Outsourcing from Europe to other parts of the world - buying security product and services on behalf of clients and have these operations in countries round the world.
Acquisition by global enterprises of specialist “domestic” security product and service companies

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

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

If you answered "other" please specify:

1200 character(s) maximum

We do not consider that there are any “missing supplies of products and/or services” on the European cybersecurity market.

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

☑ Critical infrastructures
□ Energy
□ Transport
☑ Health
☑ Finance and Banking
☑ Public Administration
□ Smart Cities
☑ Digital Service Providers
□ Protection of individual users
□ 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

Main challenges are: 1) expansion of threats (new types of threats), 2) expansion of vectors for attacks (different channels of attack), 3) insufficient pool of individual with relevant defensive / protection skills (having a workforce capable of dealing with threats). We wish to stress that the threat landscape is becoming increasingly dynamic. The nature of attacks is constantly changing, along with the repetitive nature of threats.

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

Markets in cybersecurity products/services are competitive to the extent that they are open to the global market. An open market enables innovation and allows for the integration of new services and new offerings. We believe that research funding in Europe has driven innovation, including the development of new services and products. The problem that affects competitiveness in Europe is the relative difficulty for relevant ventures to secure capital investment / funding. This is where the market is failing. Unfortunately, promising European start-ups do not receive or have access to the required levels of funding in Europe. Moreover, sometimes the expertise in cyber services from a number of Security Operations Centers that are well respected in Europe is ignored.

In terms of leadership: Europe should aspire to be a leader in research - with globally recognised institutions, in entrepreneurship with globally recognised innovation, and should build up skills and talent in Europe to develop leading companies.

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

Europe has a vibrant and successful start-up ecosystem with many SMEs expanding their offerings beyond their initial / base Member State, into other EU Member States. However, scaling-up these start-ups to become global players is a problem. We fully believe that accessing the global market is imperative to success. The European Single Market must work to provide companies with economies of scale so that they can have the potential to succeed on the global market. However, flaws continue to exist, especially resulting from national fragmentation; this fragmentation includes varied standards, different information security and product assurances, different limitations on access to public sector markets, and data localisation restrictions. We believe that a clear industrial policy is needed to counter this.

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

We believe that the European market is highly competitive because the market is open. If the market were to become more restricted, the market will likely become less competitive, as certain products and services will inevitably become inferior due to a lack of competitiveness on a global scale. In terms of weaknesses, we continue to stress the dangers associated with national fragmentation. Providing economies of scale is of central importance, and national fragmentation directly impacts this. 28 solutions rather than 1 cannot possibly remain the status quo if we are trying to prioritise “European competitiveness”. Furthermore, the suspension of cross border data flow mechanisms is a threat to the European market place as it could lead to European solutions not having access to the data they need to provide global intelligence.

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

The recently concluded Network and Information Security (NIS) Directive must be commended for refraining from encouraging high levels of local procurement and protectionism. However, the success of current and future legislation will depend upon the implementation of security measures at the Member State level. Legislation such as NIS has the potential to stimulate the market as long as implementation is successful. When it comes to the General Data Protection Regulation (GDPR), we believe that the legislation may lead the market to developing solutions that focus on not having access to data. The recent announcement of an EU-US Privacy Shield to replace Safe Harbour is welcomed, but the continued uncertainty on the future of transatlantic data flows will directly impact the European cybersecurity market in a negative way.

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 is a driver behind the cybersecurity market in Europe due to the fact that the market is open and accessible (EU public procurements are open to all tenderers, this means that any specific cybersec requirement set out in a public procurement opportunity is thrown open to be solved by tenderers located across the whole EU). However, in some limited cases, public procurement is a barrier as it is restricted and closes the marketplace to the best available products/services.

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
□ Venture funds
□ EIB/EIF support
□ Sovereign welfare funds
□ Crowd funding
□ EU funds
□ Other

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

The European ICT security and supply industry is faced with a significant skills shortage.

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

○ Yes
○ No

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

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

As previously noted, the open nature of the European market for cybersecurity products functions well. Any intervention which would add barriers and increase market fragmentation would be detrimental. Public intervention risks creating vulnerabilities as it would stop European operations from buying the best available security products. It is worth noting the value of the overall market goes beyond the acquisition of products and services. One must consider the entire supply chain (specialists, security consultants, etc.), which have a large share of the European market.

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

Capital investment remains the central issue for Europe. The continued development of a level of risk appetite and funding is needed for European companies to develop into global players. The lack of this risk level shows that there is a clear market failure. European start-ups should not need to go to 3rd countries to source capital so that they can scale-up their businesses.

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

We believe that such initiatives are counterproductive. As the nature of the cybersecurity threat landscape is global, it is counterproductive and detrimental to restrict solution sourcing to the local marketplace. In most cases this will lead to increased vulnerability, higher costs, and lower efficiency. We believe that R&D support on the national level is important as long as the marketplace remains open. Several years ago there was a tender for security products in Switzerland which was restricted to Swiss manufacturers - although there were no such indigenous manufacturers. Clearly this limits the ability of the public sector to procure the best solutions.

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

OFE monitors the development of technical specifications, standards and architectures.

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

1200 character(s) maximum

* 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

The concept of standardisation can support innovation, but only if the standards: are internationally recognised, are well-known, are industry led, and are created in response to market demand (rather than to regulatory intervention).

* 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

We believe that it is a combination between generic and sector-specific, as the application depends on each use case. Information security standards are in most cases more efficiently addressed at a generic level, but cloud-based standards are more effectively addressed in a specific manner. An example of this blend would be the healthcare sector, where there is a combination of specific standards as well as high level generic standards.

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

1200 character(s) maximum

The development of standardisation is led by industry, and occurs at an international level with strong European participation. This system has been proven to work well and as such we would discourage the introduction of specific European standardisation efforts.

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

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

○ Yes
● No

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

We believe that the work done within the European Commission Cloud Select Industry Group (C-SIG) on certification schemes has developed a robust list of successful schemes. We are of the belief that the work on identifying successful certification schemes has to be a continuous process, so that all players are aware of those schemes which have been taken up by the market and have wide geographical appeal.

*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

We wish to draw attention to the work done by ENISA on certification schemes. The certification scheme ecosystem is constantly evolving as bodies develop new schemes, but we believe the work by ENISA has proved successful and useful. We encourage the European Commission to avoid 'prioritising' any given certification scheme over any other, as competition between schemes is important for continued innovation and development.

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

1200 character(s) maximum

See reply above.

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

1200 character(s) maximum

ENISA is currently tasked with examining certification schemes, and is well placed to do this.

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

○ Yes
○ No
● I don't know

*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

Naturally, understanding this complex ecosystem is more manageable for large entities, while it is incredibly burdensome for SMEs. We point to the extensive work done by ENISA in this field. The mapping of standards and certification schemes by ENISA in collaboration with the European Commission C-SIG has proved to be a very valuable exercise, particularly for SMEs. However, we acknowledge that this work should be continued to broaden the usability of the ENISA output as standards and certification schemes can be very costly for SMEs.
Any harmonisation by existing accreditation national bodies in Europe must use the same standards and framework. The CSCG recommendation is based to provide 3 levels (minimum, substantial, and high) and to be able to harmonise the levels with other frameworks like common criteria, ISO/IEC 27000, FIPS, etc.

*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

SOGIS-MRA could be used as base, but there are government agreements to be put in place in the commercial market.

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

CSCG is currently examining labelling schemes. It will facilitate the emergence of a single cyber security market. There is a request to obtain a mutual recognition of products to ease and develop this single European security market.
The scheme foresees products and services first: complex systems or infrastructures will not be covered by such label (at least, not in a first step). A governance framework for labelling should include: certification authorities, providers, users.

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

☑ Consumer market
☑ Professional market (SMEs)
□ 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

European harmonized cyber security requirements taking into account both security and privacy issues. Different initiatives must be harmonized: e.g.: M 460, M 436, M487, M490, M530.

* 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
☑ Venture funds
☑ EIB/EIF support
□ Sovereign welfare funds
□ Crowdfunding
☑ EU funds, please specify
□ Other

* Please explain

1200 character(s) maximum

Venture finds encourage the creation of partnerships. EU funds could be used for building the skills thorugh training.

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

1200 character(s) maximum

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

Europe should aspire to be a leader in research - with globally recognised institutions, in entrepreneurship, with globally recognised innovation, and build up skills and talent in Europe to develop leading companies. All these objectives will help open up the EU market.

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

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

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	
Innovation activities	30%
Using research & innovation results to bring products and services to the market	20%
Development of national/regional cluster (or national/regional centres of excellence)	
Start-up support	10%
SME support	30%
Public Procurement of innovation or pre-commercial support of development and innovation	10%
Individual, large-scale "Flagship" initiatives	
Coordination of European innovation and research activities	
Definition of common requirements for cybersecurity products and services for specific application domains at European level (e.g. transport, energy…)	
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)
☑ Resilient Digital Civilisation (collective layer)
☑ Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)
☐ Other

*3.2. In terms of products and services

between 3 and 5 choices

☑ 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
☐ 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

☑ Critical infrastructure in general
☐ Energy
☐ Transport
☐ Health
☐ Finance and Banking
☐ Digital Service Providers
☑ Internet of Things
☑ Cloud Computing
☑ 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)

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

Please explain:

1200 character(s) maximum

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

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

☑ Support in alignment of national and European research agendas
□ Support for SMEs
□ Co-funding of national or European activities
□ Providing infrastructures for experimenting and testing
☑ Support with expertise in standardisation bodies
☑ 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 format of the NIS Platform does not require changes. The key challenge is to get wider participation in the working groups, as too many are inactive.

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

The platform should focus on Information Sharing approaches, Research and Skills.

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

Focus on information sharing was timely – contrary to top down approach of the NIS Directive.

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

```
Better information sharing is the next big challenge - but we are not
convinced that the Cyber PPP is the right vehicle for this.
```

VIII. Sharing your data and views

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

2000 character(s) maximum

```
File uploaded below.
```

Please upload your file

- **cd7ab1d9-4a3c-4a2f-83a5-f7f78ce88043/OFE Letter cPPP consultation March 2016.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