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

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

New Section

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.

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

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

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- 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

New Section

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

X 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?

X Yes

○ No

I'm responding as:

○ An individual in my personal capacity

X The representative of an organisation/company/institution

What is your nationality?

○ Austria

○ Belgium

○ Bulgaria

○ Croatia

○ Cyprus

○ Czech Republic

○ Denmark

○ Estonia

○ Finland

○ France

○ Germany

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- ○ Greece
- ○ Hungary
- ○ Italy
- ○ Ireland
- ○ Latvia
- ○ Lithuania
- ○ Luxembourg
- ○ Malta
- ○ Netherlands
- ○ Poland
- ○ Portugal
- ○ Romania
- ○ Slovakia
- ○ Slovenia
- ○ Spain
- ○ Sweden
- ○ United Kingdom

X Other

If you chose 'Other', please specify

European

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

X 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.

920867915729-68

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
- **X** European-level representative platform or association
- ○ National representative association
- ○ Research body/academia
- ○ Press
- ○ Other

If you chose "Other" please specify

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

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- ☐ Lithuania
- ☐ Luxembourg
- ☐ Malta
- ☐ Netherlands
- ☐ Poland
- ☐ Portugal
- ☐ Romania
- ☐ Spain
- ☐ Slovenia
- ☐ Slovakia
- ☐ Sweden
- ☐ United Kingdom

X Other: EU

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

European Digital SME Alliance (former name PIN-SME)

Please enter your name

Sebastiano Toffaletti

Please enter the address of your institution/organisation/business

4, Rue Jacques de Lalaing, Brussels B-1040, Belgium

Please enter your telephone

Tel: +32 22850726

Please enter your email

office@digitalsme.eu

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

The European Digital SME Alliance Secretariat : 4, Rue Jacques de Lalaing, Brussels B-1040, 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

New Section

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 "Researcher", please specify

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

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

If you answered "other", please specify

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

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- [ ] Infrastructure (network) security
- [ ] Hardware (device) security
- [ ] IT security audit, planning and advisory services
- [ ] IT security training
- [ ] Other

If you answered "other", please specify

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:

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:

II. Assessment of cybersecurity risks and threats

New Section

1. Risk identification

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

- [ ] 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)
- [x] Extraction and use of identity and payment data to commit fraud
- [ ] Intrusion in privacy
- [ ] Other

Please specify:

In order to better answer to this question it should be useful to define more clearly the definition of cybersecurity.

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

- [ ] Critical infrastructures in general
- [ ] Energy
- [ ] Transport
- [ ] Health
- [x] Finance and Banking
- [ ] Public Administration

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- [ ] Smart Cities
- [ ] Digital Service Providers

- [X] Protection of individual users
- [X] Protection of SMEs
- [ ] Other
- [ ] I don't know

Please specify:

Protection of SMEs: SMEs constitute the greatest part of the economical tissue of many countries (Italy among them). They don't have culture nor funding to protect their information so they possibly are at a greater risk than other sectors/areas, even if those ones might be of more immediate interest.

2. Preparedness

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

- ( ) Yes
- (X) No
- ( ) I don't know

If no, which are missing - please provide examples:

SMEs report criticisms about compromised hardware and "hacked chips". On the hand it is not a product/service lack, but an awareness and economical problem.

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

- [X] National/domestic supplier
- [ ] European, non-domestic supplier
- [ ] US
- [ ] Israel
- [ ] Russia
- [ ] China
- [ ] Japan

☐ South Korea

☐ Other

If you answered "other", please specify

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:

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

X Lack of economics of scale for the envisaged (national/European/global) markets

X Market barriers

☐ Other

☐ I don't know

If you answered "other" please specify:

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

☐ In the EU member state you operate

X Between EU member states

☐ Globally

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

☐ Between industry sectors

☐ Other

If you marked "other" please specify:

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)

X Critical infrastructures

☐ Energy

☐ Transport

☐ Health

☐ Finance and Banking

☐ Public Administration

☐ Smart Cities

☐ Digital Service Providers

☐ Protection of individual users

X Protection of enterprises (large companies and/or SMEs)

☐ Other

☐ I don't know

Please specify/explain

4. Cybersecurity challenges by 2020

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

These, in black, are mine answers for DIGITALSME:

1. Adaptation of Cybersecurity strategy to the needs of SMEs: simplify and adjust the directives in order to better fit the SMEs possibilities.

2. Foster Cybersecurity awareness raising actions among all stakeholders of SDM, with a particular regard for SMEs

1. Attacks on companies and economic espionage

2. Espionage on users and / or private entities hampering digitalisation

3. Developing capabilities in a joint effort to counter the threats aforementioned.

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

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

European companies have in the past proven very effective in deploying IT-Infrastructures and delivering services. However, they are behind in the development of hardware. This has proven to be a major setback for European IT-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

a) The situation for SMEs in the European Union is currently difficult. Different Data Protection Regimes, varying interests concerning data security by national governments add to the general restraints of operating in other EU countries.

b) A Digital Single Market would greatly improve the situation of SMEs offering digital security services. It would allow for a larger level playing field and for addressing larger markets. In addition to that an enhanced competition between different providers in IT security would lead to better results thus generally improving IT security in Europe.

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?

/

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)?

Lack of access to homegrown hardware.

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	☐	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 management and operation services	X	☐	☐
IT security training	☐	X	☐

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?

Fragmentation of national legislation concerning data retention and it security and definition of CRITIS, has created uproar on digital as well as non-digital markets. Companies are uncertain about impact of new legal requirements or see their business-models threatened outright through this national legislation

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

X I don't know

Please explain

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

○ Yes

X No:

There are very few dedicated initiatives, especially aimed to end users (individuals and SMEs) that normally cannot afford much security

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

☐ Bank loans

☐ Equity funds

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

- [ ] Venture funds
- [ ] EIB/EIF support
- [ ] Sovereign welfare funds
- [ ] Crowd funding
- [ ] EU funds
- [X] Other

If "other", please specify:

SMEs typically invest money of their own

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

- ( ) Yes
- (X) No
- ( ) I don't know

Please explain

There are few education path produces and few professionals in the field.

Lack of comparability of qualifications on EU Market is hampering cross border employment of qualified personnel. This will hopefully be eased through the eskills framework.

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

- (X) Yes
- ( ) No

Please describe

National legislation and fragmentation of contract law has had a generally negative impact on SMEs.

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

- (X) Yes
- ( ) No

Please describe:

Horizon 2020

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

New Section

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)

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

The main need that can be addressed at European level is establish a common cybersecurity framework and related incentives/certification schemes.

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)

Public intervention can only be detrimental since the effects it creates usually burden ICT-SME stronger than large companies. National legislation in the past has shown this.

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

N/A

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

V. Specific Industrial Measures

New Section

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?

Standardisation can generally have a positive impact for ICT companies this also holds true for the field of IT security. However, if such standardisation is undertaken it should describe basic procedures and minimum standards which allow for further development and modification through SMEs. In addition to that the standards developed should be accessible for SMEs.

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

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

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

X Yes

No

I don't know

Please explain your view

IT standards both within and outside the field of ICT Security can ameliorate the situation for ICT SMEs as innovators. When general IT standards are concerned IT security companies can build on these standards for the development and rollout of their own products. When IT security standards are concerned these can provide for both quality seals and best practices among IT security SMEs.

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)

Cybersecurity standardisation should address both sector specific approaches which are developed in cooperation with the respective industries – namely e-payment and accounting, smart energy, banking and connected traffic systems as well as IT security in general.

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

See 1.4

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

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

Yes
X No

If yes, please specify:

//

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?

ISO/IEC 27001 is the most widespread certification scheme. This as well as other existing certification schemes have proven to be loathsome to ICT SME as far as bureaucratic burdens and costs are concerned even if all security requirements are met. So when looking at certification schemes one should consider establishing simple and cost effective easy schemes adapted to the specific needs of sectors and SMEs.

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

Yes
x No
I don't know

Please explain

see 2.2

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

Partially relevant – certification schemes offer best practices and guidelines for proceeding in cybersecurity. EU wide and SME adapted solutions would be necessary.

2.5. What areas should future certification efforts focus on?

see answer 1.4

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

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

X Yes

No

I don't know

Please specify

Yes, as far as ISO/IEC standards are concerned, on which many other certification schemes are based. However, when it comes to these other certification schemes recognition is often restrained by national member states' borders.

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

Yes

X No

I don't know

Please explain

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

X Yes

No

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

Industry

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

see answers above

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

There already is a huge number of labels and quality seals available on the market. Extending these does not seem necessary unless new schemes would be specifically adapted to SMEs

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

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?

Quality of the schemes and recognition by official authorities

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

☐ Bank loans

☐ Equity funds

X Venture funds

☐ EIB/EIF support

☐ Sovereign welfare funds

☐ Crowdfunding

X EU funds, please specify

X Other

Please explain

Bank loans have recently proven to be shallow as banks have been reserved in giving loans especially to SMEs. Crowdfunding – while on the rise in public awareness often does not create the funds necessary to purposefully deploy ICT security measures which are regarded as long term measures which require permanent fostering. Public funding for ICT security – especially in the field of minimum standards for buyers – could prove helpful to apply minimum standards while venture and growth capital could help ICT SMEs to develop new applications and products and innovate cybersecurity. On the other hand "De-taxation of cybersecurity investments" is the most useful form of access to finance for European cybersecurity industry players to encourage business growth.

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

see above.

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

recognition of SME friendly applications and security solutions.

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

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?

Clusters can be helpful to disseminate cybersecurity on local or regional level.

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

A centre or hub for ICT SME to connect and collaborate on a European level could prove helpful. See page 2 of the BITMi position paper on Digital Single Market http://www.bitmi.de/custom/download/bitmi_positionspaper_digitaler_binnenmarkt_eu_1447745451.pdf

VI. The role of research and innovation in cybersecurity

New Section

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

X Yes

No

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

The European Digital SME Alliance (formerly PIN-SME) has largely participated on the side of dissemination, whose results were quite positive.

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

//

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

lack of accessibility for SMEs to participate in such projects.

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

cooperation with public authorities.

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

Tax incentives.

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

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	10
Innovation activities	20
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	30
SME support	20
Public Procurement of innovation or pre-commercial support of development and innovation	
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]

☐ Individuals' Digital Rights and Capabilities (individual layer)

X Resilient Digital Civilisation (collective layer)

☐ Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)

☐ Other

Please specify:

3.2. In terms of products and services

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

Please explain:

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

- [ ] Critical infrastructure in general
- [ ] Energy
- [ ] Transport
- [ ] Health
- [X] Finance and Banking
- [ ] Digital Service Providers
- [X] Internet of Things
- [ ] Cloud Computing
- [X] Public Administration
- [ ] Other

Please explain your choice:

see answer 1.4 in chapter 2

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

- [ ] Universities and Research Institutes

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

X 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:

SMEs are particularly challenged by national legislation as they are facing greater odds to comply

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?

see answers before

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

☐ Support in alignment of national and European research agendas

X Support for SMEs

☐ Co-funding of national or European activities

☐ Providing infrastructures for experimenting and testing

X Support with expertise in standardisation bodies

☐ Contribute to certification schemes

☐ Other

Please explain

VII. The NIS Platform

New Section

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)?

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

//

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

Question for all stakeholders

Sharing knowledge and experience

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

Question for all stakeholders

//

European Digital SME Alliance
4, Rue Jacques de Lalaing 1040, Brussels, Belgium
Tel +32 228 507 26
www.digitalsme.eu, email office@digitalsme.eu

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?

Question for all stakeholders

//

VIII. Sharing your data and views

New Section

Please upload additional data and information relevant to this survey.

[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-agenda-draft-v02.63/view