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.

52431421-12

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

If you chose "Other" please specify

Global Telecommunications Operator

My institution/organisation/business operates in:

- [ ] All EU member states

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

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

Telefonica, S.A.

* Please enter your name

Carlos Alberto Rodríguez Cocina

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

Avenue des Arts, 20 Box 7 - 1000 Brussels - Belgium

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

Gran Vía, 28 – 28050 Madrid – Spain

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?

- [x] 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

400 character(s) maximum

• Telefónica I+D participates in projects along with academia and other R&D institutions, being the innovation branch of Telefonica. Largest private R&D centre in Spain and the most active company in Europe in terms of European research projects in the ICT sector Telefonica also invests in several cybersecurity start-ups through Wayra, the Telefonica's start up accelerator in EU and Latin America

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
- [x] Other

If you answered "other", please specify

400 character(s) maximum

```
Business continuity
```

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

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

Please specify:

400 character(s) maximum

```
Telecom networks are the physical foundation of all digital networks (public
and private, Internet, VPN, etc.) and services. Telecom networks have specific
cybersecurity issues at the level of connectivity and network as well as in
other sectors identified by 2008/114/EC Directive on critical infrastructures
protection.
```

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
- [x] Other

Please specify:

400 character(s) maximum

Network Virtualisation
1 Cybersecurity has a horizontal nature. It affects different vertical solutions and services offered over the Internet or built by means of the interconnection between machines (M2M), cloud or human users
2 Embedded systems are in principle not exposed to cybersecurity threats. Those embedded systems connected to the Internet are classified in the group of IoT devices

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

* Please specify:

1200 character(s) maximum

It is difficult to limit the number of answers as for instance “extraction and use of identity and payment data to commit fraud” is also a very important topic for business, individuals, public administration and LEAs.

* 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
- [ ] Digital Service Providers

- [x] Protection of individual users
- [x] 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

-Identity & Access management solutions
-Products with an automated and holistic approach to collect and analyse information (about devices, networks, users) together with external intelligence (about vulnerabilities, threats and actors)
-Mobile and cloud services to secure the information they host and the privacy of their users
-IoT: security should be addressed by design as a design feature

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

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

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

- [x] Trustworthiness
- [ ] Interoperability of products/solutions
- [ ] Lack of European supply
- [x] Place of origin is irrelevant
- [x] Other

If you answered "other", please specify:

800 character(s) maximum

• Brand image. Trust in the solutions provided by well-known firms, and who mistrust from those European ones, even when the latter would be better and cheaper solutions that the former.
• Integration. Preferences in 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.

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
- [ ] Market barriers
- [x] Other
- [ ] I don't know

If you answered "other" please specify:

1200 character(s) maximum

o Education: lack of an official European roadmap on cybersecurity and certification training programs devoted to employees that have to deal with security IT policies and procedures. There are training gaps on (1) awareness of the risks and consequences and (2) workplace practices on proper safeguarding and cyber-hygiene
o Lack of effective instruments to funnel public and private funds devoted to product research and innovation
o Lack of regulatory flexibility of key European players that could play a bigger role in cybersecurity. For example, in the course of specific investigations or cyberattacks, telcos could benefit of a more flexible framework, for instance to (1) allow the automatic exchange of specific information (eg, IP addresses) without the need of judicial authorization, (2) exempts Telcos from administrative sanctions when good practices have been followed and (3) compel an effective collaboration of Internet application providers
o Lack of level playing field and extraterritorial effective enforcement with non-EU providers that in many cases are not subject to the same controls and provide competing security services

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
- [x] 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

-The adoption of a holistic cybersecurity approach (1) keeping pace with evolving threats, (2) coping with changing technology and business practices (innovating securely) and (3) achieving a balance between the rights of individuals and collective security. Evolve from isolated security solutions able to protect assets to products that analyse information from devices, networks, IT equipment and users together with external intelligence about vulnerabilities, threats and actors. Confidence among the industry, administrations and MSs is key for the effective implementation of this approach; cPPP play an essential role
-Pervasive schemes that enhances the security of networks. The gap between those countries that have access to high tech cybersecurity resources (ie the development of post-quantum cryptography) and others impedes to attain such goals
-Secure IoT developments. Preserve IoT trust across the whole stack (device, communication, backend and users). Overcome the lack of open standards on IoT cybersecurity or the flooding of the market with poor embedded security features. Critical infrastructures resilience could be compromised by weak cybersecurity developments of IoT

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

- Although the demand raises, the supply of European products undergoes the market dominance of cybersecurity foreign suppliers. Despite professional skills and some major European vendors, the region lacks of a solid industry able to compete with USA or Israel players.
- Non-EU products and services outstrip European ones both in number and revenue generation. User´s selection criteria can still be linked to brand names or the nationality of vendors. This might be due to the lack of European trust labels that can apply to products and also to companies.
- Non-harmonised legislations and the lack of a real single market among Member States make the commercialization expensive and difficult.
- Lack of level playing field. Vendors operating from non-European countries have a competitive advantage to those operating in a European settlement, stifling the capability of European products and services to compete.

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

- Challenging. EU based SMEs and start-ups have significant difficulties to succeed. Large companies are (1) very dependent from 3rd country-based suppliers and (2) prefer to trust in well-established brands. In fact, European IT managers generally prefer to acquire products of vendors from 3rd country-based reputed suppliers, for instance US or Israel, rather than its European equivalent ones.
- Apparently, being a vendor headquartered in the European Union does not magnify the value of a given brand and the confidence on SMEs and start-ups products. On the contrary, being stablished in 3rd regions, for instance US, does. Moreover, a vendor that provides remote data processing services, having their databases out of the EU jurisdiction could add competitive advantage caused by the lack of level playing field in EU privacy regulation.

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

- Harmonised regulations across Europe would (1) facilitate the development and marketing of products and would (2) promote the access to the single market.

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 – (1) European cybersecurity vendors generally have access to high skilled experts, good knowledge and awareness on cybersecurity threats, strong reputation in emergent markets and good level of security of the traditional service providers (i.e. telco sector). (2) EU vendors are sensitive to privacy and local regulation.
- Weaknesses – (1) EU vendors suffers a high market fragmentation, small size, lack of strong brand image, adverse regulatory framework, brain drain to third countries, (2) EU vendors have difficult access to capital. Research and innovation funds are sometimes not driven by short term market needs, (3) they experience a slow go-to-market journey and a limited scale to capture the market, (4) European start-ups have often to move to other countries to survive.

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

- Legislative measures are an important factor, for instance the NIS Directive outcome. In order to achieve a level playing field, regulation in cybersecurity should address not only those companies based in EU, but any vendor offering services to the EU, even those which do not have infrastructures under EU jurisdiction.
- In general, the legislation should tackle the cybersecurity market with similar approaches than 3rd countries does in other safety regulation (for instance to sell a car in Europe that has been manufactured abroad UE, it has to meet the safety specifications and certifications required in EU, etc.).
- Current data privacy regulation applied to cybersecurity operations is strongly fragmented and protective, hampering the collaboration in markets and products. In this respect we positively asses the Proposal on General Data Protection Regulation which 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

- On one hand, the public procurement should be the driver of a future cyber security industry in Europe. Public procurement should be one of the available instruments to produce product-driven innovation and to provide the first route to market for the resulting products, in particular if various vendors are involved to develop complex cyber-solutions. Nonetheless, public procurement is nowadays a clear barrier due to (1) the fragmentation of domestic demand of products and services and (2) the bilateral arrangements signed between each EU member state with USA or Israel companies.

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
- [x] EU funds
- [x] Other

If "other", please specify:

600 character(s) maximum

- Company funds

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

UE companies often compete for the same kind of professional profiles. Although there is a global shortage of the cybersecurity staff, the EU work force is skilled to face cybersecurity challenges .

https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

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 there are not formal barriers, the nationality of vendors can play a role to market access and export within the EU. The implementation and transposition of the European Directives causes a remarkable fragmentation of the cybersecurity market. Such lack of harmonization imposes a de facto barrier for the deployment of cybersecurity products along Europe.

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:

- From the public side, it is noteworthy the role played in Spain by the public agency INCIBE (Instituto Nacional de Ciberseguridad). In 2015, the Spanish government committed to release a 5M€ fund in 2016 for cybersecurity purposes.
- From the private sector BBVA or Telefónica have developed specific cybersecurity programs in Spain such as the "National "Antibotnet Protocol".

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 (1) human capital and (2) 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 in such areas.

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

- On regulation there is a lack of EU harmonisation, with significant differences among countries.
- On EU vendor deployment there is a need to develop (1) the cybersecurity industry, (2) creation of brands, (3) certification labels for products and services (4) certified professional careers, certified education and certified training, (5) standardization processes in the technological and management fields
- Other areas where major improvements are required are (1) programme endorsement (2) financing (3) R&D

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

Necessary.

The support at national level is necessary and useful. The market is mainly dominated by USA & Israel vendors. A way to turn this situation would be backed up by political initiatives promoted by UE Member States as a whole.
In addition, unlike other industries, cycles of implementation of R&I projects in the cybersecurity field are unusually very short, so that many products may become obsolete in a matter of months.
Such dynamic, requires that (1) the national industry of cybersecurity performs important efforts on technological innovation and (2) more flexibility to manage the changes and to deliver the required technological solutions in time.

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

1200 character(s) maximum

- The "National Antibotnet Protocol" in Spain
- The European CIP project ACDC (http://acdc-project.eu/)
- USA & Israel government endorsement programs for cybersecurity

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
Telefonica is currently involved in the SC37 standard of Biometry and also in several proposals for H2020 program related with cybersecurity, IETF (Internet Engineering Task Force) I2NSF (Interface to Network Security Function), ETSI NFV SEC (Network Function Virtualization) and TGC (Trust Computing Group). Telefonica also participates in ETSI, ITU, GSMA and ISO standardization bodies.

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

1200 character(s) maximum

Telefonica identifies a major gap in the way that the information related with cyber-incidents is shared between affected organizations. Other specific areas are, inter alia, (1) Internet of Things (IoT), (2) cryptography, (3) metrics and measurements or (4) indicators of Compromise (IoC) (i.e. STIX and TAXII standards for information exchange of threats).

* 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

- Standardization is a precondition for new comers to compete with incumbents, vendors and digital service providers in the field of cybersecurity.
- Standardisation is an outreach of the research activity. It allows to expose innovation results permits stakeholders to adopt best technical and procedure solutions.
- However, the strong and massive influence of industry big players distorts the standardization goals when they impose “de facto” standards tailored to their specific products or services.
- Moreover, the evolution of cybersecurity solutions and standards are not only driven by the adoption of new technologies but as a reaction against new cyber-threats. Such dynamic forces stakeholders to update security standards in timeframes that become unreachable to standardization fora.
- Therefore, the duration of the needed steps to publish a standard are too long to be coherent with a real innovation.

* 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

- Both. There is the necessity of framework standards that establish the objectives, general principles and criteria. A general standardization approach in cybersecurity is required at least for the sharing information in case of cyber-incidents.
- Specific sector standardization is needed although cyber-security incidents are not bounded by any particular sector. Then, a general standardization approach should be implemented in more technical details over

different fields either technical, operational or procedural security.
- Standards should be required as mandatory in the RFPs and its accomplishment necessary to operate in the market.

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

1200 character(s) maximum

- Metrics and measurements
- Indicators of Compromise (IoC)
- Privacy, secure data transfers, data sharing
- Cryptography
- IoT, Industrial Security

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

- ISO/IEC JTC 1/SC 37 on Biometrics
- ISO/IEC JTC 1/SC 23 – Digitally Recorded Media for Information Interchange and Storage

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

- Cooperation in the definition of selection criteria for cybersecurity products/solutions/services and application of European cyber guidelines and labels.
- ICT security certification schemes that would be considered successful are, inter alia (1) Security techniques on Information Security Management Systems – Requirements ISO 27001, (2) Payment Card Industry Data Security Standard PCI DSS, (3) 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 scale. They will drive the EU to a blockage if each stakeholder distrust to other ones.
- Security certification schemes are very expensive and time consuming processes. The EU should face and reverse this situation urgently.

* 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 in cybersecurity products and services to build trust within the single market. Creation of a list of cross-certified which guarantees that national certifications are applicable to equivalent products need to be pushed at EU level in particular for public procurement to obtain a “trusted supply chain”.

* 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

- ISO standards

* 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

- In general, certification is very time consuming and costly. A convergence of certifications would certainly help users to better understand common requirements and vendors.
- The inclusion of trusted third parties involved in (1) the assessment of compliance with standards or other reference and (2) the mapping of various certifications and labels would make easier the equivalence between standards, certification schemes and labels.

* 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

- Telefonica refers mainly to the industry schemes, for instance ISO 27001, 15408, FIPS. However it is urgent to create new labelling schemes that overcomes the challenges and threats that current ones are facing.
- Self labelling schemes provide little value for customers or buyers of cybersecurity products.

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

800 character(s) maximum

- Current labeling schemes have high visibility for buyers. However, those labels lack of efficiency and readability.

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

1200 character(s) maximum

- Essential. It is key to develop the resilience of the supply chain providing essential services to citizens and companies. As there are already many certification schemes, the goal would not be creating new labels but to expand approaches and ensure some convergence among the existing ones.

* 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

- Endorsement of labels and use by Public Administration as early adopter would be an important element for further success
- The involvement of a trusted third party
- Ease of use, visibility
- Efficiency in cost and time consumption
- It would be urgent to extend labelling schemes to include new challenges and ensure convergence.

* 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

- EU funds devoted to research programs

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

1200 character(s) maximum

- (a) Start-ups should receive the support of endorsement programs to promote the purchase of start-ups products in equal conditions than other equivalent ones available in the cybersecurity market from vendors of 3rd regions. It would allow European start-ups to scale-up without the need long term funds.
- (b) Set-up R&D programs to share (a) university resources (the entrepreneurs), (b) public/private funding (the capital) and (c) the private endorsement of the outcome by customers (the products).

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 (1) foster consumption of products and services manufactured by EU companies, (2) create and invest in cybersecurity brands, (3) foster competitive price/quality EU products, (4) harmonise regulation across the EU and provide homogenous and 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 centers of excellence play its own role as a starting point in fostering industrial policies in the field of cybersecurity, although they lack of the international shaping. In particular, they have a positive effect on skills, growth and human development. Such clusters should focus on the development of skilled work force and wider security awareness.
- Duplication of efforts among them should be avoided by means of the adequate coordination mechanisms. The islands of know-how or any kind of internal market barriers have to be prevented.

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

R&I European programmes provided a valuable knowledge to Internet Service Providers on cybersecurity procedures and products. They also helped to national PPP programs (e.g. CIP ACDC). The key outcomes were on the area of the Network Architectures Validation for ISPs (e.g. SECURED FP7).

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

1200 character(s) maximum

The main impacts of projects funded in cybersecurity were (1) the improvement of user awareness (2) malware reduction in networks and (3) on standardization results the launching of new Working Groups.

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

1200 character(s) maximum

The key shortcomings were:
- Difficulty to bring the results into applications. Lack of applicability and reuse of the program outcomes by the Business Units in Telefonica.
- Long cycles from innovative ideas to commercial products: slow innovation process and lack of significantly sized demonstration and commercialisation actions to accelerate transfer from laboratory to market.
- Lack of testbed facilities. Lack of possibility to work with real data.
- Slow / non harmonised standardisation and certification.
- Insufficient EU and MS funding to support emergence of EU solutions in strategic sectors. Dispersed use of R&I funding without a comprehensive strategy.

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

1200 character(s) maximum

The PPP should contribute to (1) define harmonised R&I priorities, (2) an increased in the competitiveness of EU solutions developing and implementing measures for a cybersecurity industrial policy, (3) coordinating activities for standardisation and certification (including test and validation facilities) and (4) the support, definition and implementation of EU legislative measures for specific sectors. Project clustering in the cPPP would facilitate the share of data and the results in order to enrich projects by collaboration.

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

1200 character(s) maximum

To set-up national consortia that would simplify the bureaucracy for the participation of SMEs in such programmes and would generate synergies between the involved companies. For instance, in Spain INCIBE (“Instituto Nacional de Ciberseguridad”) facilitates the integration of SMEs around a technological pole or cluster.

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	25%
Using research & innovation results to bring products and services to the market	25%
Development of national/regional cluster (or national/regional centres of excellence)	5%
Start-up support	5%
SME support	
Public Procurement of innovation or pre-commercial support of development and innovation	
Individual, large-scale "Flagship" initiatives	
Coordination of European innovation and research activities	5%
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

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

* 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
- [x] Digital Service Providers
- [x] 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)

- [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 interrelated. Global players allow more impact in different national markets.
- Innovation at Europe level must be a task developed in such a coordinated manner involving all the active players.
- Without a proper educational infrastructure and a network of research centres it would not be possible to define a continuous stream of talent to feed the set-up of start-ups and to allow the enterprises to innovate.

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

To stimulate SMEs competitiveness, the following needs would require further developments:

- Link cybersecurity SMEs with their innovative products to concrete needs. Use sectoral SME clusters as a mechanism at local level and beyond (Regional/Member State) to develop the market.
- Enhance the skills on cybersecurity by investing in professional and educational training programs in universities and research centers.
- Promote the user awareness on cybersecurity and the strategic implications of protecting information and storage systems.
- Reinforce the involvement of governmental institutions in response to the strategic nature of the cybersecurity in terms of financial and operational support for the development of cybersecurity solutions.

* 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, precisely, 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 in line with the guidelines produced by ENISA on the implementation of art. 13.a. of the Framework Directive. Considering that the scope of the NIS Directive is larger than the scope of Art. 13.a., this will require intensive work of all stakeholders.

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

Cybersecurity is critical to ensure digital trust and enhance customer digital experience to achieve a thriving digital economy. Users and companies have to reach a balance between security strength, quality and affordability. New security requirements will imply major investment efforts.
The NIS Directive will contribute to a higher level of cybersecurity in Europe, achieving a LPF by setting out cybersecurity obligations for operators of essential services and for digital service providers. A higher degree of harmonization of risk management has to be achieved across the EU.
The proposal of a Cybersecurity cPPP will (1) help to overcome the barriers for the consecution of a Digital Single Market for Cybersecurity products, (2) help to address market gaps while supporting the development of a robust European cybersecurity industry and (3) enhance cross-sectorial cooperation

between telecommunications and other sectors.
For the cPPP to succeed, it is important to stress the specificity of the ICT/Telco sector, because, as primary users of cybersecurity products and also part of the supply side, it should be present with a special weight in the governance of the cPPP. Telefónica is committed to build a thriving European cybersecurity market and to foster trust and bottom-up cooperation on R&D among Member States and the ICT/Teleco industry.
Some issues to be highlighted in the future cPPP to avoid former mistakes, are (1) build trust between Member States and other stakeholders (2) create a role of Chief Security Officer with official certifications (3) support SMEs/start-ups with endorsement programs to guarantee that their products/services will be bought by Public Administrations and (4) promote research in a wide range of fields.
There is also need for the development of (1) tools and standards for Security Evaluation (Common Criteria) and Certification and (2) metrics for an objective and systematic evaluation of security products/services.

Please upload your file

[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