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.

64270747023-20

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
- [x] 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.

DIGITALEUROPE

* Please enter your name

Damir Filipovic

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

14 rue de la Science, 1040 Brussels

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

Brussels, Belgium

Consultation

Note:

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

I. Identification of your priorities in cybersecurity

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

- [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

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

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

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

2.1. Dedicated Cybersecurity -> Cybersecurity products/services

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

If you answered "other", please specify

400 character(s) maximum

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

- [x] Critical infrastructures in general
- [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

Manufacturing is an area of growing relevance considering security. This area of IoT and especially Industry 4.0 will demand specific requirements on security and safety.

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

- [x] Internet of Things
- [x] 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

II. Assessment of cybersecurity risks and threats

1. Risk identification

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

between 1 and 3 choices

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

* Please specify:

1200 character(s) maximum

It is unclear what is meant by 'intrusion in privacy'. We take the view that the term 'privacy' goes beyond personal privacy. We are left to assume that this describes the security of essential data of an entity against unauthorised access. If so, an 'intrusion' may impact the reputation, image, competitive advantages and knowledge of an entity.

Furthermore, we would recommend including building awareness of cyber threats and the necessity of encouraging cyber-hygiene best practices such as patching and phishing education, network segmentation, and multi-factor authentication/identity management in relation to risk management (as included in CERT-EU guidelines).

* 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
- [x] Energy
- [ ] Transport
- [x] Health
- [x] Finance and Banking
- [x] 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

Many of the above sectors can be classified as critical infrastructure making the selection of some sectors repetitive. Also, 'Digital Service Providers' is

not an appropriate sector classification. We also question why 'defence' and 'manufacturing' have been omitted. Both of these sectors face frequent cybersecurity risks.

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?

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

If you answered "other", please specify

200 character(s) maximum

Cybersecurity products and services are selected from a global market based on their competitiveness. An open market place will ensure innovation and the creation of competitive solutions.

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

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

If you answered "other", please specify:

800 character(s) maximum

We believe this question must be viewed from an understanding of the global nature of the marketplace. When one closely looks at cybersecurity solutions, they typically go through 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. Furthermore, it is worth noting the importance that companies play in buying security products and services on behalf of their clients who have operations around the world. Examples include i2 (Cambridge, UK) and QRadar (Belfast, Northern Ireland). These European companies have a global scale of operations.

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

If you answered "other" please specify:

1200 character(s) maximum

We do not think there are missing cybersecurity supplies of products and/or services on the European 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

- [x] Critical infrastructures
- [x] Energy
- [ ] Transport
- [x] Health
- [x] Finance and Banking
- [x] 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

We wish to note once more that many of the above sectors can be classified as critical infrastructure making the selection of some sectors repetitive. While a serious cybersecurity incident could lead to significant damage in many of the above mentioned areas, we are of the opinion that a serious cybersecurity incident in critical infrastructures, as defined in the Network and Information Security (NIS) Directive, is most likely to cause the worst socio-economic damages.

4. Cybersecurity challenges by 2020

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

1200 character(s) maximum

1) Expansion of threats (new types of threats) and vector for attacks (different channels of attack) - This will require enshrining cyber-hygiene best practices (e.g. patching/phishing education, network segmentation, and multi-factor authentication/identity management, as recommended by CERT-EU) This is of particular importance for the IoT environment, where ensuring the security of various devices and objects which connect to a data centre will be a challenge. Securing mobile devices, particularly as corporates move to mobile cloud is also of importance as vectors increase.

2) Operational excellence (effective infrastructure) - Increasing complexity will lead to increasing investment and cost to deal with threats. If market conditions do not enable the required investment, security will drop steadily.

3) Skills (having a workforce capable of dealing with threats) - Today, 35% of organisations say that they have open security positions that they are unable to fill, according to “The State of Cybersecurity: Implications for 2015”, a study by ISACA. As operation technology and information technology continues to converge, this issue will continue to become more acute.

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. Examples of successful European HQ cybersecurity companies include: BT (security and risk management solutions), Sophos (anti virus/ malware), DFLabs (incident and breach response), DeepSecure (content

control & inspection), SentryBay (PC, mobile & IoT security), AVG Technologies (antivirus/ internet security SW), ClearSwift (data loss prevention).

The problem that affects competiveness in Europe is capital investment / funding of ventures. This is where the market is failing. Unfortunately, promising European start-ups do not receive the right levels of funding in Europe.

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 Member State to the other Member States of the EU. 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 become successes on the global market. However, flaws continue to exist in the form of national fragmentation. This fragmentation includes varied standards, different information security and product assurances, limitation to accessing public sector markets, and data localisation restrictions. We believe that a clear EU led industrial policy is needed to counter this. To solve this problem Europe should aspire to be a leader in research – with globally recognised institutions, in entrepreneurship – with globally recognised innovation, and in talent – by building up the skills which can be harnessed to develop leading companies.

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

We wish to stress that the openness of the market in Europe will have a direct bearing on R&D investment in Europe. We firmly believe that if the market is closed/limited the incentive to invest in Europe will decline leading to an uncompetitive economic environment for the development of cutting edge cybersecurity products/solutions.

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 become inferior due to a lack of competitiveness on a global scale. In terms of weaknesses, we continue to stress that national fragmentation is a weakness. Providing economies of scale is of central importance and national fragmentation directly impacts this. 28 solutions rather than 1 should not remain the status quo. Furthermore, the continued risk of suspension/restricted use of certain 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 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 at the Member State level, particularly as it relates to adopting an international approach to security requirements on essential operators and digital service provides and avoiding additional national requirements on product testing and security. 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. Measures should be taken to assure an approach balancing access to data and privacy taken by industry. Moreover, the announcement of an EU-US Privacy Shield to replace Safe Harbour is welcomed, but the continued uncertainty on the future of international data flows (particularly 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. However, in some limited cases, public procurement is a barrier as it is restricted and closes the marketplace to the most suitable 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?

- [x] Bank loans
- [x] 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

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

We firmly believe that the European ICT security and supply industry is faced with a significant skills shortage. (ISC)2, the security certification and industry body, notes in its 2015 Global Information Security Workforce Study that there will be a shortfall of 1.5mil security professionals by 2020. Other reports have indicated that this skills gap could last through to 2030. The UK Government's 2014 Cyber Security Skills Report notes that skills related to implementing secure systems, followed by operational management, incident management and information risk management are among the cyber security skills most in demand from the private sector. Some government initiatives, such as that of the UK Government, are a positive step to addressing this issue, but more must be done on a European level.

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

Following recent terrorist attacks, cybersecurity has been placed as a high priority for many governments around the world. This has led to policies which directly impact market access including mandatory technology transfers requirements, local sourcing requirements in government and private sector procurement, the escrow of source code and other sensitive design elements, import restrictions and restrictions on the flow of data. These policies conflict with international norms (Article XIV of GATS), but also jeopardise sectoral growth. Examples where barriers exist include China (Anti-Terror Law, draft cybersecurity law, guidelines for banking and insurance sector), Vietnam (Network Information Security Law), South Korea (national intelligence service guidelines on cloud computing), and India (requirements for in-country testing and certification of products with compulsory registration order).

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

As examples we wish to highlight the Hague Security Delta in the Netherlands (security cluster bringing together businesses, government and academia), the UK National Cyber Security Programme (includes elements such as the Cyber Innovation Centre in Cheltenham and the Early Stage Accelerator Programme), and the Finnish National Cyber Security Innovation Programme.

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 (i.e. most suitable) 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 third 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

As the nature of the cybersecurity threat landscape is global, any national initiatives must be well crafted so as not to cause increased vulnerability, higher costs and lower efficiency, which are outcomes from market closures. An

example of such an activity was a recent tender for security products in Switzerland which was restricted to Swiss manufacturers although there were no such indigenous manufacturers. We believe that R&D support on the national level is important as long as the marketplace remains open so that suppliers are not excluded based on nationality. Any national or European level activities should be done in a cooperative manner to avoid duplication while keeping in mind the overarching idea that the cyber landscape is global.

We believe that the European approach started with the NIS initiative is more adequate generating a Single market overcoming the market fragmentation due to national initiatives and interventions.

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

1200 character(s) maximum

V. Specific Industrial Measures

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

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

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

1200 character(s) maximum

Yes, industry is currently working with standards related to cybersecurity. We wish to emphasise, that these standards are well-known and mature international standards with a proven track record in the international market place providing for economies of scale. These include ISO 27000 series and a range of technical standards such as X.805, PCI, OWASP, etc. from a variety of bodies such as 3GPP, ETSI, ISO, IETF, and NIST.

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

1200 character(s) maximum

As mentioned in previous questions, we believe that that a robust portfolio of international standards currently exists that have been proven in the marketplace and as such there is a minimal need. We believe the work done by the European Network and Information Security Agency (ENISA) within the

European Commission Cloud Select Industry Group (C-SIG) has proven a useful exercise in mapping out the international standards for cybersecurity in the cloud computing arena. We encourage such exercises as they aid SME's in identifying workable international standards.

* 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 and aid market growth, rather than stifling it, but only if they are internationally standards that are well-known, industry led, and respond to market demand rather than regulatory intervention. However, standardisation is only part of the broader puzzle when it comes to innovation and the digital single market. Much of what happens in the world of cybersecurity does not always fit into recognised standards, which is why standardisation processes must remain industry led. Moreover, we wish to stress that the correlation of standards fostering a true DSM remains unclear at the moment.

* 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 standards is led by industry and occurs at an international level with strong European participation. This system has proven to work well and as such we discourage the introduction of European standardisation efforts. In all fields where the ICT industry innovates, cybersecurity must be an integral part of any 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

* If yes, please specify:

600 character(s) maximum

Many of our members are active in certification bodies. Once more we would like to point to the Commission's C-SIG on certification schemes for cloud computing where many industry players were active and participated. Our members are also actively contributing to the cybersecurity assurance efforts in 3GPP SECAM (Security Assurance Methodology) and the related GSMA NESAS (Network Equipment Security Assurance Scheme) as well as the on-going activities of CEN and ETSI.

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 in the previously mentioned Commission C-SIG on certification schemes has developed a robust list of successful schemes. We are of the belief that the work to identify successful certification schemes is a continuous process. It is important for all industry actors, regardless of size, to be 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

Once more, we wish to draw attention to the work done by ENISA on certification schemes within the Commission C-SIG. The certification scheme ecosystem is constantly evolving as bodies develop new schemes, but we believe the work done by ENISA has proved successful and useful. We encourage the Commission to avoid 'prioritising' a given certification scheme over others 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

The relevance of certification schemes is based on the understanding the certification scheme ecosystem. Understanding this ecosystem is manageable for large entities, but incredibly burdensome for SMEs. We again point to the work done by ENISA in this field to alleviate the complexity for SMEs. The mapping of certification schemes by ENISA has proven to be a very valuable exercise. However, this work should be continued to broaden the usability of the output as certification schemes can be very costly for SMEs.

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

1200 character(s) maximum

We are of the opinion that future certification efforts should continue to focus on identifying successful certification schemes as they come to market. We commend the work done by ENISA on identifying existing certification schemes and believe they are well placed to continue this process for the benefit of all industry players.

* 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

Certification schemes which are successful and have proven themselves in the marketplace are recognised widely across the EU’s Member States. However, those schemes which are widely recognised and successful are those which have global application rather than only European application. The EU will continue to benefit from certification schemes which have a proven global track record rather than limiting themselves to an EU applicability.

* 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

As previously noted, understanding the complex ecosystem of standards, certification schemes and labels is manageable for large entities, but incredibly burdensome for SMEs. We point to the work done by ENISA in this field to alleviate the complexity for SMEs. The mapping of standards and certification schemes by ENISA within the Commission's C-SIG has proven to be a very valuable exercise. However, this work should be continued to broaden the usability of the output as standards and certification schemes can be very costly for SMEs.

We further wish to note that further harmonisation of accreditation bodies in Europe is recommended so that the same standards and frameworks can be recognised across the EU. To build this harmonisation the CSCG issued recommendations based on 3 levels (minimum, substantial and high) in an effort to harmonise European activities with other frameworks such as ISO/ISEC 27000.

Furthermore, we wish to emphasise that existing national standards not yet included in the European framework must be included as per the Vienna/Dresden agreement when relevant and justified. National existing standards could be taken into considerations via ISO/IEC.

* 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

We wish to draw attention to the work being done by CSCG to examine labelling schemes. It will cover low, significant and high security level requirements with the aim to facilitate the emergence of a single cyber security market for Europe. We believe that SOGIS/MRA could be used as a platform for harmonising labelling schemes across Europe through an industry-led manner, but believe that government agreements will need to be put in place for this to work on 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

Professional buyers, due to their maturity, can do an assessment of labels from a business-to-business point of view. As we represent globally operating companies we would welcome the availability of globally recognised options. Furthermore, while we do not rule out the possibility of the creation of labels that have value for those entities with less maturity, but we are not aware of any successful cases for developing labels for consumers or SMEs.

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

1200 character(s) maximum

As we represent globally operating companies we would welcome the availability of globally recognised options. The lack of mutual recognition for labels makes them ineffective in raising security levels. Moreover, we wish to note that along with being unaware of any successful cases for labelling, we believe the main obstacle to successful labelling is the absence of any methodologies that would enable reliable and repeatable labelling techniques that could be useful to consumers and apply to a reasonably broad range of products. We believe this could be an area to investigate from an R&D perspective.

* 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?

1200 character(s) maximum

We believe that harmonised European cybersecurity requirements taking into account both security and privacy issues will be critical for the success of any labelling schemes. We believe that different initiatives across the EU Member States must be harmonised including actions surrounding M460, M436, M487, M490 and 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

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

* Please explain

1200 character(s) maximum

We have approached this question from the point of view of the start-up market. As such, we stress that it is important that there is access to funding for Europe's start-ups and SMEs so as to allow them to continue to

provide innovative cybersecurity products. Investment in security infrastructure is key to regional development and as such should be the target of EU funding.

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

1200 character(s) maximum

We believe that the continued development of innovation hubs has proven successful, but we also wish to stress that connecting existing innovation hubs is important. Many hubs are rooted in a government partner and as such are national by nature. Creating a network affect amongst these hubs could lead to increased collaboration of cybersecurity start-ups in Europe.

We also believe that national governments have a role to play in the education sphere so that essential cybersecurity skills are taught at an early age. Educations schemes such as Cyber Essentials in the UK should be used as a model.

Lastly, increased access to venture capital is critical for start-ups looking to scale-up across the EU market and beyond. Increasing the flow of capital to start-ups is of paramount importance for their growth. This also connects closely to developing a culture in the EU around acquisition amongst start-ups in their journey to scaling-up.

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

We wish to stress that all Member States are covered by the Wassenaar arrangement and EU Regulations on export control on conventional arms and dual use goods and technologies, including cybersecurity products and services. As such, we encourage the Commission to support closer cooperation from an authorised licensing perspective so that the export of products with low security concerns can be easily facilitated. The export of less sensitive products broadly available at the global level could be eased by Community General Export Authorisations. Certifications required for security features for some environments are lengthy and expensive, and at variance with shortening product development cycles. This must be avoided to enhance exports and we call for greater harmonisation between Member States of practices and procedures when it comes to export controls.

Furthermore, avoiding market fragmentation is of critical importance. While cybersecurity is an important national issue, some sectors (e.g. healthcare) become very local in their approach. This must be avoided.

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

Cybersecurity clusters have proven effective for the development of EU cybersecurity products and services as a pooling of expertise has led to the exchange of practices and more competitive products and services. We continue to stress that it is important for SMEs across Europe to consolidate to enhance their exporting potential.

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

Access to flexible, short-term funding opportunities could better match the nature of technological efforts in the cybersecurity space. Financial measures should also be defined to support multidisciplinary studies. We also wish to stress once more that Europe should aspire to be a leader in research – with globally recognised institutions, in entrepreneurship – with globally recognised innovation, and in talent – by building up the skills which can be harnessed to develop leading companies. The institution of policy instruments focusing on these issues will work to support the development of the European cybersecurity industry.

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

We are unable to answer on behalf of our members for specific projects as they vary greatly and have differing outcomes

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

1200 character(s) maximum

We are unable to answer on behalf of our members for specific projects as they vary greatly and have differing outcomes

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

1200 character(s) maximum

We are unable to answer on behalf of our members for specific projects as they vary greatly and have differing outcomes

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

1200 character(s) maximum

We are unable to answer on behalf of our members for specific projects as they vary greatly and have differing outcomes

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

1200 character(s) maximum

We are unable to answer on behalf of our members for specific projects as they vary greatly and have differing outcomes

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	20
Innovation activities	20
Using research & innovation results to bring products and services to the market	5
Development of national/regional cluster (or national/regional centres of excellence)	10
Start-up support	5
SME support	5
Public Procurement of innovation or pre-commercial support of development and innovation	5
Individual, large-scale "Flagship" initiatives	10
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…)	15
Other (please specify)	0
TOTAL (100%)	100

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

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

between 2 and 3 choices

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

* 3.2. In terms of products and services

between 3 and 5 choices

- [x] 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
- [ ] IT security management and operation services
- [ ] IT security training
- [ ] Other

Please explain:

600 character(s) maximum

While we are restricted to 5 choices, we believe that “IT security management and operation services” should be included, particularly when considering threat intelligence & detection and cyber defence in an industrial context.

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
- [x] Energy
- [ ] Transport
- [x] Health
- [x] Finance and Banking
- [ ] Digital Service Providers
- [ ] Internet of Things
- [ ] Cloud Computing
- [x] Public Administration
- [ ] Other

Please explain your choice:

1200 character(s) maximum

We believe that many of the above sectors can be classified as critical infrastructure making the selection of some sectors repetitive. Also, while we are once more limited to 5 choices, we would have liked to also select that “Internet of Things”.

Furthermore, as previously noted, while a serious cybersecurity incident could lead to significant damage in many of the above mentioned areas, we are of the opinion that a serious cybersecurity incident in critical infrastructures, as defined in the NIS Directive, is most likely to have the highest impact on society and as such should be the priority of European support actions.

We continue to stress that we are of the opinion that ‘Digital Service Providers’ is not an appropriate sector classification. We also question why ‘defence’ and ‘manufacturing’ have been omitted from the list of sectors that could benefit from European support actions. Both of these sectors face frequent and significant cybersecurity risks.

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
- [ ] 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

As previously noted, the problem that affects competitiveness in Europe is investment into SMEs and start-ups. We believe that European research and innovation efforts should be focused on these players as they are in many instances where such players fail to receive the right level of support from the market.

Furthermore, Europe should aspire to be a leader in research, and should have globally leading university and research institutions. As such, European research and innovation activities should focus on this subset as well.

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

Once more, we wish to stress that national fragmentation is a weakness and a barrier for innovative SMEs to stimulate competitiveness. Providing economies

of scale is of central importance and national fragmentation directly impacts this. 28 solutions rather than 1 should not remain the status quo. The EU should continue to limit national fragmentation whenever possible.

* 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

DIGITALEUROPE and our members are active in all of the above mentioned activities. We firmly believe that a combination of the above is the role that industry must play to contribute to fostering innovation and competitiveness of cybersecurity products and services in Europe. We pledge to continue this work and our activities moving forward.

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

We believe that for the platform to become more effective, certain aspects must be improved with a specific emphasis placed on achieving a more outcome orientated approach. Unfortunately, the long term role of the Platform was vague. This led to unclear deliverables in many Working Group (particularly WG1 & 2 with the exception of WG3 on Research and Innovation) and a mix of individuals in meetings (engineers, lawyers, government affairs), which at times became a hindrance to achieving progress. Any future activities should be built on a preliminary open discussion with stakeholders to identify clear goals and measurable deliverables.

The second improvement is that wider participation in the Working Groups is needed in the future as there were too many inactive observers. Particularly noteworthy was the low number of SME and Member State officials active in the platform. We believe the unclear objectives and general participation were potentially a cause for this.

Lastly, the governance structure lacked clarity and transparency. If the Platform is to continue, different partners, such as ENISA, are better positioned to drive some of the originally envisioned outcomes.

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

We believe that the NIS Platform should focus on information sharing particularly when it comes to approaches on developing research programmes and skills enhancement. Furthermore, the NIS Platform should play a role in providing advice on the implementing security measures of the NIS Directive. This should include incident reporting, coordination between public bodies, and the identification of constraints for technologies and solutions for public administrations, public sector entities and consumers. Furthermore, as mentioned above, we believe different partners, such as ENISA, are better position to drive some of the future work streams of the Platform should it continue.

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

DIGITALEUROPE engaged in the NIS Platform as we thought its creation was timely and promised a good platform for exchanging information between

stakeholders. We wish to emphasise that the focus on information sharing was timely and a strong reason for engaging. We strongly believe in the public-private cooperation model and continue to do so. However, as previously mentioned, the Platform suffered from a number of flaws, highlighted by the lack of a clear understanding of the long term objectives. This was coupled with the mix of participants with a large majority acting as silent observers rather than participants. This was a reason for not participating. Furthermore, we wish to voice our disappointment at the slow drop in participation of Member State officials as the promise of public-private cooperation was one of the main expected benefits of the Platform.

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

As we have noted previously, our motivation for engaging in the NIS Platforms' work after the adoption of the NIS Directive will be continued information sharing amongst participants and the ability to engage directly with ENISA, the Commission and Member State officials on the implementation of the Directive. We acknowledge though that this will become a challenge once the NIS Directive is fully implemented. However, we continue to see the value in the NIS Platform for this purpose, despite the challenge, as we are not convinced that the Cyber PPP will become the correct mechanisms for such information sharing in the future. Instead we believe that the Platform should encourage a collaborative system amongst all stakeholders including the creation of a governance model where participants elect the leadership and direction of the Platform.

VIII. Sharing your data and views

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

2000 character(s) maximum

We wish to stress that when it comes to cybersecurity, what is most important is the protection provided by a solution, rather than the specific geographical origins of a solution. We urge caution against the implementation of policies within the field of cybersecurity that focus on any goal other than the effective protection against threats. These threats are today global in nature and will remain so regardless of their target or origin. We are concerned about some questions within this consultation which ask organisations about their reasons for choosing "non-European ICT security products/services over European ones". We wish to stress that the origin of a security product or service should not play a role in judging its effectiveness or performance.
We fully support the strengthening of the EU's ability to produce competitive cybersecurity products and services. The EU should continue to work to attract

investment and resources to develop and strengthen this sector of the economy. However, this should not be done by displacing (or substituting) non-European solutions from the Single Market. Doing so risks lowering Europe's protection from cybersecurity threats as the highest quality products, regardless of their origin, should be available on the marketplace to provide for effective protection. Defending European cyberspace requires a global mindset, not isolation. Isolation risks higher threat exposure, weaker defences, and the inability for European players to scale up at the rate necessary to become competitive.

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