

# 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](mailto: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.**

Global6214521205

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

Swiss not-for-profit organization

My institution/organisation/business operates in:

- All EU member states

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

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

Global Legal Entity Identifier Foundation (GLEIF)

\* Please enter your name

Stephan Wolf

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

Baumleingasse 22, 4015 Basel, Switzerland/Bleishstrasse 59, Frankfurt am Main, Germany

\*

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

Germany

## Consultation

---

Note:

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

### I. Identification of your priorities in cybersecurity

---

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

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

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

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

If you answered "other", please specify

*400 character(s) maximum*

Public/Private Partnership

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

2.1. Dedicated Cybersecurity -> Cybersecurity products/services

- Identity and access management
- Data security
- Applications security

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

If you answered "other", please specify

*400 character(s) maximum*

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

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

Please specify:

*400 character(s) maximum*

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

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

Please specify:

*400 character(s) maximum*

## II. Assessment of cybersecurity risks and threats

---

### 1. Risk identification

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

*between 1 and 3 choices*

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

- \* Please specify:

*1200 character(s) maximum*

The need to protect the correct identity information so that users can rely on knowing their counterparties.

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

*between 3 and 5 choices*

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

Please specify:

*400 character(s) maximum*

### 2. Preparedness

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

- Yes
- No
- I don't know

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

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

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

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

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

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

### 3. Impact

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

*between 1 and 5 choices*

- Critical infrastructures
- Energy
- Transport

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

Please specify/explain

*1200 character(s) maximum*

Unique entity identification based on the Global LEI system is a prerequisite to protect the above-mentioned areas from damage based on incorrect entity information.

#### 4. Cybersecurity challenges by 2020

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

*1200 character(s) maximum*

Economic sabotage, Identity theft, System disruption

### 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*

No opinion.

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*

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

GLEIF is a global operating Swiss foundation with excellent access to the European market via its German branch office.

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

No opinion.

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	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
*Data security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
*Applications security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
*Infrastructure (network) security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
*Hardware (device) security	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
*IT security audit, planning and advisory services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
*IT security management and operation services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
*IT security training	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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

Legislation being enacted in the EU relying on usage and accuracy of Legal Entity Identification will demand that this information remain correct and secure.

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*

Examples in other parts of the world indicate that public demand can stipulate innovation and growth in IT/security.

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

- Yes
- No

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

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

If "other", please specify:

*600 character(s) maximum*

GLEIF is funded by fees from LEI issuance. The Global LEI system is under oversight by 70 international financial regulators. Twenty international organizations have observer status in the Regulatory Oversight Committee. See more on <https://www.gleif.org/en/about>

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

- Yes
- No
- I don't know

Please explain

1200 character(s) maximum

The industry is not acting fast enough on skill management. Universities do not focus enough on industry demands. Certification is falling behind. Many experts come therefore from abroad.

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

- Yes  
 No

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

- Yes  
 No

## 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

Data privacy protection

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

Identity management through the LEI can be a positive contributor to the success of the Digital Single Market. The LEI would bridge the digital economy with real world identity management. The LEI already is mandated by European regulators in the area of Finance. An extension to capture digital identity would be advisable and beneficial for European enterprises and consumers.

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

More regulation on a European scale is needed to overcome national barriers and standards. Identity management being most important in this space.

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

*1200 character(s) maximum*

Counterparty identification in Europe through MiFID/MiFIR regulation in the Finance area. Important for risk management and protection on a global scale.

## 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*

No, GLEIF is not currently working on these as GLEIF relies on its suppliers in the area of cybersecurity.

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

*1200 character(s) maximum*

In the near term, GLEIF is going to engage with standards organizations and technology providers to embed the LEI in digital identity management. For instance, the LEI could become of source of validation for digital certificates.

\* 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*

Standards are a prerequisite for any international technology adoption. Standards such as ISO 17442 are the foundation for public goods where the industry failed to deliver scalable solutions with no barrier to access.

- \* 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*

There should be foundational standards and each sector should review and apply these standards as necessary for the particular sector.

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

*1200 character(s) maximum*

Finance, Internet trade, identity threats

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

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

- Yes  
 No

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

*1200 character(s) maximum*

Not applicable

- \* 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*

Not sufficient in the area of identity management.

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

*1200 character(s) maximum*

Very important. See Extended Validation Certificates as an example.

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

1200 character(s) maximum

Identity management

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

- Yes
- No
- I don't know

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

- Yes
- No
- I don't know

Please explain

1200 character(s) maximum

They rely on each other; they are not equivalent.

\* 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

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

1200 character(s) maximum

No opinion

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

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

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

1200 character(s) maximum

No opinion

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

*between 1 and 5 choices*

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

\*Please explain

*1200 character(s) maximum*

All of the above. Focus should be on private equity and venture capital.

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

*1200 character(s) maximum*

No opinion

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*

No opinion

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*

No opinion

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*

Mandating the LEI as a standard for identity management above and beyond the Finance sector.

## VI. The role of research and innovation in cybersecurity

---

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

Yes

No

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

	% (specify 0-5-10-15-25-50-100)
Fundamental research	
Innovation activities	
Using research & innovation results to bring products and services to the market	
Development of national/regional cluster (or national/regional centres of excellence)	
Start-up support	
SME support	
Public Procurement of innovation or pre-commercial support of development and innovation	No opinion
Individual, large-scale "Flagship" initiatives	
Coordination of European innovation and research activities	
Definition of common requirements for cybersecurity products and services for specific application domains at European level (e.g. transport, energy...)	
Other (please specify)	
<b>TOTAL (100%)</b>	

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

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

*between 2 and 3 choices*

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

\* 3.2. In terms of products and services

*between 3 and 5 choices*

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

Please explain:

*600 character(s) maximum*

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

*between 3 and 5 choices*

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

Please explain your choice:

*1200 character(s) maximum*

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

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

Please explain:

*1200 character(s) maximum*

No opinion

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*

No opinion

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

- Support in alignment of national and European research agendas
- Support for SMEs
- Co-funding of national or European activities
- Providing infrastructures for experimenting and testing
- Support with expertise in standardisation bodies
- Contribute to certification schemes
- Other

Please explain

*1200 character(s) maximum*

Contributing to secure identification management by developing the Global LEI System.

## 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 (NISIP).

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*

No opinion

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*

No opinion

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*

GLEIF was not aware of the NIS platform until this questionnaire.

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 previously stated, GLEIF is relying on its providers for cyber security.

## VIII. Sharing your data and views

---

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

*2000 character(s) maximum*

Not applicable

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](mailto:CNECT-FEEDBACK-CYBERSECURITY-DSM@ec.europa.eu)

---