Questionnaire on the evaluation and review of the European Union Agency for Network and Information Security (ENISA)

Fields marked with * are mandatory.

Background

More than 70% of EU citizens access the internet daily, and most of them use digital devices for a range of activities including communication, shopping, work and administration. Information systems, which are key to the functioning of modern economy and society, can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. They can have a direct impact on citizens, but also disrupt the functioning of businesses and public organizations, including those providing essential services (like energy, healthcare, and transport), generate substantial financial losses for the EU economy and negatively affect societal welfare. Digital information systems work across borders. A disruption incident in one EU country can have a direct or indirect impact on other Member States or the EU as a whole.

The EU seeks to protect citizens, Member States and businesses' from cybersecurity incidents, through regulatory, policy and technological tools. The European Union Agency for Network and Information Security Agency (ENISA) was founded in 2004, to contribute to this effort, by helping the EU institutions, Member States and the business community in addressing network and information security issues. Its current objectives, mandate and tasks were set in 2013 by the Regulation No 526 /2013 (ENISA's Regulation) for a seven year period, until 2020.

Your Voice Matters: with this consultation the European Commission seeks views of experts and stakeholders to evaluate ENISA's overall contribution to the cybersecurity landscape for the period 2013-2016. With this public consultation the Commission seeks input from citizens, professionals and organizations from all EU countries and all professional and cultural backgrounds.

The legal basis for the evaluation is found in Article 32 of Regulation (EU) No 526/2013, which foresees the commissioning of an evaluation of ENISA's activities by June 2018.
The results of this public consultation will also be used as input to prepare the ground for a possible renewal and/or revision of the Agency's mandate.

You are welcome to answer the questionnaire in its totality or limit your contribution to one of the two areas of the consultation:

- Backward looking – ex-post evaluation of ENISA – see evaluation roadmap
- Forward looking – focusing on evolving needs and challenges in the cybersecurity landscape and possible role of a EU body to meet them in future; this part will help the European Commission choose policy options for a possible revision of ENISA's mandate

The European Commission would like to underline the importance of this consultation in shaping the future cybersecurity landscape in Europe. Your views are essential to this exercise.

HOW TO SUBMIT YOUR CONTRIBUTION
You are invited to fill in the online questionnaire available below. The questionnaire is only available in **English**, but you can submit your contribution in any EU official language.

Please read carefully all the accompanying documents, including the reference documents, personal the data protection rules and the privacy statement, before filling in the questionnaire.

Please submit your contribution to this public consultation at the latest **by 12 April 2017.**
All queries on the process should be addressed to the email address: **CNECT-FEEDBACK-ENISA@EC.EUROPA.EU**

In the interest of transparency, organisations (e.g. NGOs and businesses) are invited to provide the public with relevant information about themselves by registering in the Transparency Register and subscribing to its Code of Conduct. If you are a registered organisation, please indicate the name of your organisation and your Register ID number, in your contribution. Your contribution will then be considered as representing the views of your organisation. If your organisation is not registered, you have the opportunity to register now. After registering your organisation, please return to this page to submit your contribution as a registered organisation. The Commission will consider responses from organisations not registered as those of individuals and publish them under that heading.

We will publish all contributions on the Commission website and your answers will be accessible by the public. This is a necessary part of a public consultation. It is important that you read the privacy statement attached to this consultation for information on how your personal data and contribution will be dealt with.

*Fields marked with * are mandatory. In addition to your responses, you may upload a document (e.g. a position paper). This is possible at the end of the questionnaire.*

You may pause at any time and continue later. Once you have submitted your answers, you can download a copy of your completed responses.

Please note that only responses received through the online questionnaire will be taken into account and included in the report summarising the responses.
Questionnaires sent by email, on paper, or in other formats will not be analysed.

BACKGROUND NOTE

Background_document_ENISA_PC.pdf

SPECIFIC PRIVACY STATEMENT

ENISA_Privacy_statement_Public_consultation.pdf

The questionnaire as a Word file.

The questionnaire available via this online tool is the reference questionnaire. This file is only meant as an aid in filling in the online version. Please note that only responses received through the online tool will be taken into account and included in the report summarising the responses.

ENISA_review_Word_questionnaire.docx

Information about the contributor

*** You are replying:**

- ○ as an individual in your personal capacity
- ○ as an individual in your professional capacity
- ◉ on behalf of an organisation

*** Please provide us with your first name:**

Maika

*** Please provide us with your last name:**

Föhrenbach

* **Please provide us with your email address.** Your email address will not be published on the Commission website.

If you do not have an email address, please write “Not available”.

maika.fohrenbach@amchameu.eu

* **What is your country of residence?**

Belgium

* **Your contribution:**

Note that, whatever option you have chosen, your answers may be subject to a request for public access to documents under Regulation (EC) N°1049/2001.

- (●) can be published *with your personal information* (I consent the publication of all information in my contribution in whole or in part, including my name or my organisation's name, and I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent publication.)
- ( ) can be published *provided that you remain anonymous* (I consent to the publication of any information in my contribution in whole or in part (which may include quotes or opinions I express, provided that it is done anonymously. I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.)

* **Name of your organisation:**

American Chamber of Commerce to the EU (AmCham EU)

* **Postal address of your organisation:**

Avenue des Arts 53, 1000 Brussels, Belgium

* You are answering on behalf of an organisation or in a professional capacity, **which type of organisation is that**:

- ( ) Private enterprise
- ( ) Professional consultancy, law firm, self-employed consultant
- (•) Trade, business or professional association
- ( ) Non-governmental organisation, platform or network
- ( ) Research and academia
- ( ) EU institution or bodies
- ( ) National authority
- ( ) CERT/CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team)
- ( ) Other

* **What sector do you work in?**

- ( ) Key Internet company (e.g. large cloud providers, social networks, e-commerce platforms, search engines)
- ( ) Energy
- ( ) Transport
- ( ) Health
- ( ) Financial sector
- ( ) Telecom sector
- ( ) Cybersecurity
- ( ) Hardware manufacturer
- ( ) Software development
- (•) Other

* If "other", please specify the sector:

```
Cross-sectoral association representing members from all of the above
```

* How many employees does the company have?

- ( ) More than 250 employees (Large enterprise)
- ( ) Between 50 and 250 employees (Medium-sized enterprise)
- (•) Between 10 and 49 employees (Small enterprise)
- ( ) Less than 10 employees (Micro enterprise)
- ( ) Self-employed (Micro enterprise)

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

- (•) Yes
- ( ) No
- ( ) Not applicable

* Please give your organisation's registration number in the Transparency Register.

5265780509-97

* **Please indicate the country of your organisation's/institution's headquarters/main seat:**

Belgium

* **Are you a representative of ENISA's Executive Board, Management Board, Permanent Stakeholder Group, or of the National Liaison Officer network?**

- ( ) Yes
- (•) No

Questions

The questionnaire is divided in two parts:

- **Backward looking – focusing on ex-post evaluation of ENISA. Based on the evaluation roadmap, the aim is to assess the relevance, impact, effectiveness efficiency, coherence and EU added value of the Agency having regard to the period 2013-2016**
- **Forward looking – focusing on the needs and challenges in the cybersecurity landscape and the possible role of a EU body including policy options for a revision of ENISA's mandate.**

* Please indicate what section(s) you wish to contribute to:
You can choose either one section or both, and will be redirected accordingly.

- [x] Section 1 Backward looking
- [x] Section 2 Forward looking

Backward looking

The following questions concern your experience with ENISA's products and services, and your assessment of ENISA's overall contribution to Network and Information Security in the EU.

* In the period 2013-2016, how frequently did you interact with ENISA or used ENISA's products and services?

- ( ) On a weekly basis
- ( ) On a monthly basis
- (•) A few times per year
- ( ) One to two times per year
- ( ) Never

* In the period 2013-2016, did you use any of the following products developed or services offered by ENISA? Please tick only those products/services which you have used. (You can choose more than one answer.)

- [x] Guidelines & recommendations, including on standards
- [ ] Training or workshop opportunities
- [x] Reports (e.g. NIS Threats Landscape) and Research Publications
- [ ] The Cyber Europe Exercise
- [ ] Article 14. requests (Specific requests for advice and assistance from the EU institutions or Member States)
- [ ] Training material or toolkit
- [x] Events
- [ ] Technical advice, including to support policy development and/or implementation
- [ ] Other (please specify)
- [ ] None

* Why did you decide to use these products/services? (You can choose more than one answer.)

- [ ] The products and services are of high quality
- [ ] The products and services provide unique information (not offered by other bodies or organisations)
- [x] The products and services are provided by an EU-level body
- [ ] The products and services provide information that is independent and neutral
- [x] The products and services are free of charge
- [x] The products and services can be trusted
- [ ] The products and services are easily understandable (in terms of the terminology and language used)
- [ ] The products and services are easy for me to find and access
- [ ] Other reason
- [ ] I don't know

How relevant were these products/services to your work/activities?

	Very relevant	Relevant	Somewhat relevant	Not relevant
*Guidelines & recommendations, including on standards	○	○	◉	○
*Training or workshop opportunities	○	○	○	◉
*Reports (e.g. NIS Threat Landscape) and Research Publications	○	◉	○	○
*The Cyber Europe exercise	○	○	○	◉
*Article 14. requests (specific requests for advice and assistance from the EU institutions or Member States)	○	○	○	◉
*Training material or toolkit	○	○	◉	○
*Events	◉	○	○	○
*Technical advice, including to support policy development and /or implementation	○	○	○	◉
Other	○	○	○	○

* **Did ENISA's products and services over 2013-2016 respond to the emerging needs of the cybersecurity community in a timely manner?**

- ○ Yes, to a large extent
- ◉ Yes, to some extent
- ○ Yes, to a small extent
- ○ No, not at all
- ○ I do not know

* **Are there any other products and/or services that you would have liked ENISA to provide the cybersecurity community with over 2013-2016?**

- ○ Yes
- ◉ No

To what extent do you consider that ENISA has achieved the following objectives over 2013-2016?

	To a great extent	To some extent	To a limited extent	Not at all	I do not know
*Developing and maintaining a high level of expertise in cybersecurity	◉	○	○	○	○
*Supporting the development of EU policy	○	◉	○	○	○
*Supporting the implementation of EU policy	○	◉	○	○	○
*Supporting the EU institutions, agencies and bodies to strengthen their capability and preparedness to prevent, detect and respond to network and information security problems and incidents	○	◉	○	○	○
*Supporting the Member States to strengthen their capability and preparedness to prevent, detect and respond to network and information security problems and incidents	○	○	◉	○	○
*Supporting cooperation in the cybersecurity community, e.g. through public-private cooperation, information sharing, enhancing community building, coordinating the Cyber Europe exercise	○	◉	○	○	○

* What do you perceive as ENISA's main achievements over 2013-2016? You may include specific examples.

• ENISA has constructively helped to promote cyber issues to the top of the European policy agency and to keep them there.
• ENISA has become a visible and highly respected center of expertise in the cyber domain.
• ENISA has demonstrated clear European added value.
• ENISA has produced substantial deliverables that are practical and useful for policy makers as well as for cyber practitioners (e.g. Incident notification for Digital Service Providers in the context of the NIS Directive and Technical Guidelines for the implementation of minimum security measures for Digital Service Providers).
• ENISA has remained true to the spirit of public-private partnership and cooperation so important to cyber.

* Over 2013-2016, in what areas do you consider that ENISA could have done better? You may include specific examples.

The crucial importance of a high level of regulatory coherence in the cyber domain remains underestimated across Europe. Ideally a fully harmonised threat-informed and risk-based approach towards cybersecurity should be promoted in order for cybersecurity not to become (or remain) a fragmenting factor within the European Digital Single Market. ENISA has already done a lot to help in that regard, and AmCham EU hopes that moving forward the Agency will further contribute to efforts in this direction.

* **To what extent are ENISA's activities coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of your organisation?**

- (●) Yes, to a large extent
- ( ) Yes, to some extent
- ( ) Somewhat, but to a small extent
- ( ) No, not at all
- ( ) I do not know

* **To what extent are ENISA's activities coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of its stakeholders, including other EU agencies and bodies?**

- ○ Yes, to a large extent
- ◉ Yes, to some extent
- ○ Somewhat, but to a small extent
- ○ No, not at all
- ○ I do not know

* During 2013-2016 ENISA had its offices located in two sites in Greece, namely Heraklion (Headquarters and administration) and Athens (Operational staff). **Did this arrangement affect ENISA's ability to conduct its work effectively and efficiently?**

- ○ Yes, to a large extent
- ○ Yes, to some extent
- ○ Yes, to a small extent
- ○ No, not at all
- ◉ I do not know

* ENISA today has 84 staff members. **Do you consider that the size of the agency is adequate for the work entrusted to it?**

- ○ Yes, completely adequate
- ○ Yes, partially adequate
- ◉ No, partially inadequate
- ○ No, completely inadequate
- ○ I do not know

* To conclude this section, **please give your overall assessment of ENISA for the period 2013-2016.**

- ○ Very good
- ◉ Good
- ○ Fair
- ○ Poor
- ○ Very poor
- ○ I don't know

Forward looking

1- What are the needs and the gaps within the current and future cybersecurity landscape in Europe?

Since 2013, when ENISA's mandate and objectives were last reviewed, the cybersecurity landscape has evolved significantly, in terms of the threat landscape, and technological, market and policy developments. These developments include policy and regulatory measures, in particular those set out in the 'NIS Directive' and the 2016 cybersecurity Communication, where ENISA will and/or could play a role (see background document).

The following questions aim to determine what the needs and gaps are in the cybersecurity landscape in Europe from today's perspective and looking ahead to the next ten years.

* Considering the evolving cybersecurity landscape and current EU policy response, **what will be the most urgent needs or gaps in the cybersecurity field in the EU in the next ten years?** (You can choose up to 5 answers.)

at most 5 choice(s)

- [ ] Capacity to prevent, detect and resolve large scale cyber attacks
- [ ] Protection of critical infrastructure from cyber attacks
- [ ] Protection of the large companies from cyber attacks
- [ ] Protection of SMEs from cyber attacks
- [ ] Protection of citizens from cyber attacks
- [ ] Protection of government bodies from cyber attacks
- [x] Cooperation across Member States in matters related to cybersecurity
- [ ] Capacity to prevent, detect and address hybrid threats (combining physical and cyber)
- [x] Cooperation and information sharing between different stakeholders, including public-private cooperation
- [ ] Civil-military cooperation
- [x] Awareness within society of the importance of cybersecurity
- [ ] Innovative IT security solutions
- [ ] Standards for cybersecurity
- [ ] Certification schemes for cybersecurity
- [ ] Research, knowledge and evidence to support policy action
- [x] Skills development, education, training of professionals in the area of cybersecurity
- [x] Other (please specify below)
- [ ] I do not know

* Please specify the need/gap:

```
Effective international cooperation especially with strong allies like the U.
S.
```

* Please elaborate on your answer on needs/gaps:

Cybersecurity threats and challenges are multi-jurisdictional with no adherence or recognition of national boundaries. Often the attacker is in a separate country from the victim firm, which again is in a separate country from the customers' of the victim firm who are impacted by the attach. However the public policy approaches to tackle them often tend to be very disjointed, especially with many governments considering cybersecurity threats are domestic in nature, as a matter of sovereign and exclusive national security competence. While this is understandable it is highly damaging to the effort to develop effective collective defence responses and the broader ability to develop true cyber resilience. More cooperation is needed between nations, including between Member States of the EU, as well as between public sector actors and private stakeholders, especially businesses producing cyber-relevant technologies and the industries using them. To effectively tackle cyberattacks, further developing Member State cooperation within the EU, international cooperation between the EU and third countries particularly in the Transatlantic relationship (through, and also above and beyond the existing EU-U.S. Cyber Dialogue), and all useful forms of public-private partnership at the local, national, European and international levels as well is of fundamental importance.

Moreover, cybersecurity being a matter of people, process and technology where quite often the human element is indeed the weakest, proper awareness raising across the European society at large, as well as dedicated education and specialized training will be essential for the EU to be equipped with the necessary quantity and quality of skilled cyber professionals successfully and sustainably to manage future cyber challenges.

* **Are the current instruments and mechanisms at European level e.g. regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies adequate to promote and ensure cybersecurity with respect to the above mentioned needs?**

- ○ Yes, fully adequate
- ◉ Yes, partially adequate
- ○ No, only marginally adequate
- ○ Not at all
- ○ I do not know

Please elaborate on your answer on current instruments and mechanisms:

In the 2013-2016 timeframe the EU has made unprecedented progress to set up its regulatory and institutional framework for cybersecurity. The cybercrime directive (2013/40/EU), the eIDAS regulation, the second payment services directive (PSD2), the fourth anti-money laundering directive (AML4), the General Data Protection Regulation (GDPR), the law enforcement data protection directive (2016/680) and the Network and Information Security (NIS) directive all got adopted, and the European Cybercrime Centre was created in that timeframe. Moreover a comprehensive review of the European telecommunications framework, including the ePrivacy directive, is underway, and the recently proposed revision of the EU's dual-use export control regulation is also meant to be extended to cyber surveillance technologies. All these instruments combined provide an already very comprehensive regulatory and institutional framework around the cybersecurity of digital information, infrastructure, identities and interactions.

However the majority of these instruments are still in the process of being implemented, some have yet to enter into force, and others are still in the making. Before any further regulatory or legislative action is undertaken, it is highly recommended to let the current actions play out fully, to let the newly created institutions and structures settle in, to give the new instruments the chance to prove their worth and effectiveness, and, if and where necessary, to make fine-tuning adjustments through the existing transposition, implementation and enforcement mechanisms that already exist. ENISA has a role to play in many of these areas, in particular to support the implementation of the NIS Directive and of the eIDAS regulation, as well as to provide cybersecurity related advice and guidance to supervisory authorities, data controllers and data processors to put in practice the security and breach notification requirements of the GDPR.

In the next couple of years, stability, predictability and legal certainty will be more important than ever for the business community to be able to adapt to the new regulatory environment and to devise, validate and implement the compliance strategies, cooperation mechanisms and business models and processes through which this regulatory and institutional environment for cybersecurity can contribute effectively to the growth and to the competitiveness of the European Digital Single Market. AmCham EU members are looking forward to cooperating in particular with ENISA towards these objectives.

* In order to address the identified needs or gaps in future, **what should be the top priorities for EU action from now on in the area of cybersecurity?** (You can choose up to 3 answers.)

at most 3 choice(s)

- [ ] Further strengthening the EU legislative and regulatory framework
- [x] Stronger EU cooperation mechanisms between Member States, including at operational level
- [ ] Improving capacity in Member States through training and capacity building
- [ ] Improving education and curricular development in cybersecurity
- [x] Improving research to address cybersecurity challengesStronger public-private cooperation in cybersecurity
- [ ] Stronger cooperation between different authorities and communities (e.g. between CERTs and law enforcement authorities; ISACs and CERTs)
- [ ] Awareness raising and providing information to EU citizens
- [ ] Stronger cooperation between civil and military cybersecurity authorities and organisationsImproved monitoring of threats and incidents across Member States
- [ ] Harmonised framework for security certification of IT products and services
- [ ] Harmonised sectoral standards
- [ ] Support to the development and supply of innovative IT security solutions by the market
- [ ] Strengthening support to Small and Medium Enterprises (SMEs), including their access to financing
- [x] Other
- [ ] I do not know

* Please specify the other top priority:

```
Stronger transatlantic cooperation and regulatory convergence
```

Please elaborate on your answer on the top priorities:

Our three top priorities are:
- Stronger EU cooperation mechanism between MS, including at operational level
- Stronger public-private cooperation in cybersecurity
- Stronger transatlantic cooperation and regulatory convergence.

As explained earlier, the existing regulatory and institutional environment around cybersecurity in the European Union is already fairly substantial, detailed and comprehensive. This gives to the business community operating in the European Digital Single Market both a clear indication of the way forward in terms of identifying and leveraging cybersecurity related opportunities for innovation and growth, and a considerable set of compliance tasks to absorb.

At the same time cybersecurity is by far not only (and perhaps not even mainly) an issue of market regulation. Security in cyberspace is first and foremost a matter of trust: trust between citizens, businesses and governments, as well as trust between governments themselves, whether within the EU, or between the EU, its constituents and third countries. Many cyber issues such as the definition of acceptable norms of state behaviour in cyberspace, international cooperation to combat cybercrime, collective and cooperative defence against cyber and hybrid threats as well as the advancement of regulatory convergence belong to the realm of intergovernmental dialogue and cooperation and should be addressed at that level.

AmCham EU members are very strongly committed to supporting such dialogue and cooperation, in particular the pursuit and deepening of the EU-U.S. Cyber Dialogue, but would caution against any approach that would try to resolve difficulties or tensions encountered in the intergovernmental area by putting unfair or unreasonable compliance burdens on businesses. A particular case in point is the importance of NOT palliating the lack of intergovernmental consensus on matters like national security and intelligence operations or law enforcement mutual assistance in cyberspace through regulatory measures that would unduly force public authorities' access to confidential business records. Such measures would not only undermine public trust and confidence in businesses, their products and their services, but they could also critically undermine the foundations of network and information security, and thereby exacerbate cyber threats to citizens, businesses as well as governments.

2- The possible role of an EU body in the future EU cybersecurity landscape.

The following questions seek to ascertain whether an EU body, such as ENISA, has a role to play in the future cybersecurity landscape in the EU and, if so, what should it be.

* Given the gaps and needs identified above, **do you think there is a role for an EU-level body in improving cybersecurity across the EU?**

- (●) Yes
- ( ) No

* Do you see a future role for **ENISA** in addressing the gaps and needs identified?

- (●) Yes
- ( ) No

Given the gaps and needs identified above, **to what extent could ENISA fulfil a role in bridging these gaps, if sufficiently mandated and resourced in future?**

	To a high extent	To some extent	To a limited extent	Not at all	I do not know
*Further strengthening the legislative and regulatory framework at EU level	( )	(●)	( )	( )	( )
*Stronger EU cooperation mechanisms between Member States, including at operational level	( )	(●)	( )	( )	( )
*Improving capacity in Member States through training and capacity building	( )	( )	(●)	( )	( )
*Improving education and curricular development in cybersecurity	( )	( )	(●)	( )	( )

*Stronger cooperation between different authorities and communities (e.g. between CERTs and law enforcement authorities; ISACs and CERTs)	○	○	◉	○	○
*Stronger public-private cooperation in cybersecurity	◉	○	○	○	○
*Improving research to address cybersecurity challenges	○	◉	○	○	○
*Awareness raising and providing information to EU citizens	◉	○	○	○	○
*Stronger cooperation between civil and military cybersecurity authorities and organisations	○	○	○	◉	○
*Improved monitoring of threats and incidents across Member States	○	◉	○	○	○
*Harmonised framework for security certification of IT products and services	○	○	◉	○	○
*Harmonised sectoral standards	○	◉	○	○	○

*Support to the development and supply of innovative IT security solutions by the market	○	◉	○	○	○
*Strengthening support to Small and Medium Entreprises (SMEs), including their access to financing	○	◉	○	○	○
Other	○	○	○	○	◉

* Please specify the other role you envisage:

N.A.

* Please provide some examples of what ENISA's role could be, the competences it would require, e.g. regulatory powers or operational competences.

Any sub-optimal harmonization of cybersecurity-related regulatory requirements across the European Digital Single Market will inevitably lead to market fragmentation, lost economies of scale, increased compliance costs, hindrances to innovation, entrepreneurship and trade, loss of European competitiveness in the global market, as well as, possibly, lesser practical cybersecurity outcomes to benefit European citizens, businesses and governments. ENISA has developed the necessary good reputation, inclusive openness and authoritative expertise to weigh in credibly on policy discussions in that area. While the EU's room for manoeuvre to further integrate the single market in the area of cybersecurity remains a politically sensitive matter, a stronger, better resourced and consequently more effective ENISA could be instrumental in fostering a more harmonious implementation of existing cyber security policies and regulations across the various Member States, for example by promoting the definition of harmonious implementing measures, technological standards and technical specifications where such are mandated by existing legislation like the eIDAS regulation of the NIS Directive.
Moreover, ENISA could also be further empowered and resourced to become the standing institutional custodian of cyber-policy dialogue between EU policy makers, the private sector and civil society, to become a center of excellence for developing awareness raising, education, training and exercising resources, to be an authoritative and neutral point of reference for cybersecurity good practices and benchmarking, and perhaps even to start offering capacity building and capability validation services on a commercial basis, whether to public or private sector customers.

What other EU initiatives, if any, could be put in place to address the gaps and needs identified? E.g. legislative initiative, financial programme?

The EU will need to invest considerably more into addressing the cyber skills gap, from basic education and hygiene to the professional qualification and advanced training of skilled and specialised cyber work force. This could be achieved through existing activities (e.g. European Cyber Security Month (ECSM). Other regions of the world have also realized this need and very fierce competition is to be expected both to attract and retain the existing expertise, and to train the next generations with sufficient proficiency and in sufficient numbers. If Europe can manage to be an early and fast mover in that area, it can greatly contribute to Europe's competitiveness in the global race. On the contrary, should Europe lag behind, its exposure to cyber threats could greatly increase and its resilience against them be dramatically impaired. AmCham EU members are investing very heavily in Europe and view the long term and abundant availability of high quality cyber expertise as key for the success and sustainability of their investments in the region, as well as a prerequisite for the safe, secure and reliable growth of Europe's digital economy more generally.

Document upload and final comments.

Please feel free to upload a document. The maximal file size is 1MB. Please note that the uploaded document will be published alongside your response to the questionnaire which is the essential input to this public consultation. The document is optional and serves to better understand your position.

If you wish to add further information - within the scope of this questionnaire - please feel free to do so here.

Contact

CNECT-FEEDBACK-ENISA@EC.EUROPA.EU