Contribution ID: cc04ab3f-ac64-4ca2-b502-66cc1f7afa07
Date: 12/04/2017 12:20:19

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:**

Damir

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

Filipovic

* **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”.

damir.filipovic@digitaleurope.org

* **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:**

DIGITALEUROPE

* **Postal address of your organisation:**

14 rue de la Science, 1040 Brussels

* 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:

DIGITALEUROPE represents the digital technology industry in Europe and our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. These companies fall within more than one of the fields 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.

64270747023-20

* **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.

☑ Section 1 Backward looking
☑ 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.)

☑ Guidelines & recommendations, including on standards
☑ Training or workshop opportunities
☑ 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
☑ 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)
□ The products and services are provided by an EU-level body
□ The products and services provide information that is independent and neutral
□ The products and services are free of charge
☑ 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.

During the 2013-2016 timeframe, DIGITALEUROPE believes that one of the main achievements of ENISA was its positive contribution to the Cloud Select Industry Group (“C-SIG”) particularly the launch of the ‘Cloud Certification Schemes List’ (“CCSL”) and the ‘Cloud Certification Schemes Metaframework’ (“CCSM”). We firmly believe that activities such as these provide added value to European industry and adds much needed transparency to help customers with procurement of cloud services. We would encourage the development of similar activities in the future.

Furthermore, we believe the work of ENISA related to the Network and Information Security ("NIS") Directive, specifically ENISA’s approach to solicit input into its non-binding guidelines on incident reporting and minimum security baselines for Digital Service Providers ("DSPs") was a positive achievement. We would encourage continued involvement of ENISA into the development of the NIS Directive implementing acts as the technical expertise provided by the agency is a positive contribution to the EU policy making process.

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

During the 2013-2016 time frame, while DIGITALEUROPE welcomed the work of ENISA for its development of the CCSL and CCSM, we would encourage the agency to focus on various verticals beyond those that have been addressed thus far. The expansion of work into other verticals and industry sectors would provide the entire European economy with the awareness and capacity building that is required to address the emerging cyber threat landscape.

More broadly speaking, we would suggest that ENISA expand their consultation process by ensuring that they consult on ALL their projects - potentially through their website. That would allow ENISA to receive more feedback and improve the end products.

Moreover, there continue to be gaps between ENISA's technical expertise and the political understanding of cybersecurity by the relevant stakeholders in the European Commission. This has been evident on several occasions. Here are three examples:
1. The limited understanding ENISA has shown with regard to the 'light touch approach' for DSPs in the context of the NIS Directive, which resulted from the fact that the teams writing the NIS guidelines were not exposed to the political discussions during the negotiations on the Directive;
2. Conversely, the lack of uptake of the ENISA work on NIS ultimately received from the Commission in the development of the NIS implementing acts; and
3. One two other important issues, namely IoT security and labelling as well as on security standards and certifications, the Commission seems to trust newly created organisations such as AIOTI over the expertise it has (or in principle should have) 'in-house' within ENISA.

Ultimately, these are not necessarily areas ENISA could have done better on its own - it rather speaks to the need for the Commission to better include ENISA in the policy making process as well as broaden its resources in order to ensure proper expertise across a broad spectrum of issues can be delivered by the agency.

* **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 <u>your organisation</u>?**

○ 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

* Please elaborate on your answer on the location of the offices:

DIGITALEUROPE believes that ENISA being located at two sites in Greece has had a direct impact on capacity building. During the 2013-2016 time frame ENISA unfortunately lost some technical expertise following some staff departures. We believe that even when ENISA is able to replace those staff members which have left, the agency should seek to expand its current base of technical expertise by hiring more staff with deep technical expertise. We believe that if ENISA was located at a major European hub and avoided a ‘split’ office structure it would be easier to recruit more high quality staff members.

* 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
☑ Cooperation across Member States in matters related to cybersecurity
□ Capacity to prevent, detect and address hybrid threats (combining physical and cyber)
☑ Cooperation and information sharing between different stakeholders, including public-private cooperation
□ Civil-military cooperation
□ 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
□ Skills development, education, training of professionals in the area of cybersecurity
□ Other (please specify below)
□ I do not know

* Please elaborate on your answer on needs/gaps:

DIGITALEUROPE believes that harmonised standards and the implementation of globally common ICT security standard frameworks have become more pressing issues to tackle in order to help European businesses meet their commitments when it comes to cybersecurity and regulatory compliance.

Within the EU, there remains a risk of the proliferation of inconsistent approaches and national policies. Although DIGITALEUROPE does not believe ENISA should lead on the development on EU wide standards, we do believe that ENISA should play a role in 'keeping track' of Member State developments in an effort to point out where divergences with international standards occur. Furthermore, ENISA should work to promote internationally agreed upon standards and frameworks to ensure that fragmentation caused by the promulgation of national standards does not occur.

DIGITALEUROPE also believes that effective cybersecurity is about the ability to effectively and efficiently prevent, detect, and respond to attacks. A significant amount of cybersecurity risks and business losses can be avoided by the deployment and adoption of "cyber-hygiene" best practices of least privilege access, such as patching and phishing education, network segmentation and automation, and multi-factor authentication/identity management in relation to risk management. Increasing awareness of cybersecurity best practices is an important step for all businesses (including startups and SMEs) as well as consumers in order to enable trust in the digital age.

Lastly, when it comes to the protection of critical infrastructure from cyber-attacks, this is indeed a concern for DIGITALEUROPE, but it should be for EU-CERT to tackle. The role of ENISA should be instead to support from a technical guidance perspective.

* **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:

As previously mentioned, we would encourage ENISA to focus on various verticals in an effort to increase cybersecurity awareness and capacity building, as well as the adoption of cross-sectoral best practices. One good example was ENISA's work to explore cloud security approaches for the financial sector with the aim to promote cloud adoption in the vertical. More work similar to this project (which was carried out in partnership with EBA) is strongly encouraged. Furthermore, in light of the recent attention being paid by the European Commission on the impact of cybersecurity risk in the sphere of IoT, we would encourage more work on this field to provide the European Commission with the much needed evidence and potential impacts of any legislative actions within the field of IoT.

Lastly, we would recommend that the different instruments and mechanisms mentioned in the question are compared/contrasted and would also recommend the examination of different incentives available to encourage greater adoption of cybersecurity best practices.

* 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

☐ 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

☐ 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

☐ Other

☐ I do not know

Please elaborate on your answer on the top priorities:

As mentioned above, we encourage ENISA to focus activities on various verticals. We believe that industry sectors could benefit from increased engagement with ENISA particularly if certification and standards are applied horizontally across vectors in an effort to build up cybersecurity resilience. As previously noted, we believe ENISA has a clear role in tracking developments at the national level and encouraging harmonisation while informing the cybersecurity community of divergence. We would caution against ENISA obtaining the role of driving new certification or standards.

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

DIGITALEUROPE believes that ENISA could have a larger role in developing cooperation with third countries, specifically third country CERTs. While European cybersecurity policy making tends to focus (understandably) on European concerns, the cybersecurity landscape is global in nature and as such a stronger emphasis on the importance of the international aspects of cybersecurity would be welcomed.

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

DIGITALEUROPE believes that one of ENISA’s strengths is its role in communication and capacity building across the EU. We believe ENISA should continue to take the lead in identifying, understanding, preventing and responding to cyber threats in Europe. For example, there are certain best practices and “cyber-hygiene” activities, which governments and companies can encourage to reduce the threat vector. ENISA played a key role in promoting and enshrining such best practices in its products and services (e.g. by including the concept of network segmentation in its technical guidelines for the implementation of minimum security measures for DSPs). We believe that ENISA’s role should continue to be central to support effective EU policy-making in this area.

Closely related to this is supporting training and educational activities in the field of cyber defence in order to establish and sustain highly-trained practitioners in Europe, particularly in European public administrations and critical infrastructure.

Furthermore, as previously mentioned, we believe a continued involvement of ENISA within the field of cyber standardisation could aid in creating the best conditions for a uniform and controlled dissemination of European cybersecurity standards.

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