Contribution ID: 37061628-d563-4787-9a52-93fb56eb04f4
Date: 10/04/2017 17:54:32

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:**

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

* **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".

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

Netherlands

* **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:**

Cyber Security Directorate - Ministry of Security and Justice - The Netherlands

* **Postal address of your organisation:**

PO Box 20301 2500 EH Den Haag

* 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

* Please specify the type of national authority.

- ○ National parliament
- ○ National government
- ◉ National authority or agency
- ○ Regional or local authority (public or mixed)
- ○ Other

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

- ○ Yes
- ○ No
- ◉ Not applicable

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

Netherlands

* **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.)

- [x] Guidelines & recommendations, including on standards
- [x] Training or workshop opportunities
- [x] Reports (e.g. NIS Threats Landscape) and Research Publications
- [x] The Cyber Europe Exercise
- [ ] Article 14. requests (Specific requests for advice and assistance from the EU institutions or Member States)
- [x] Training material or toolkit
- [x] Events
- [x] 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
- [x] 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
- [x] 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)
- [x] 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

If yes, please specify the product or service:

> Benchmark/overview of duties of care, best practices public private cooperation and more a broker function of ENISA to make visible what expertise and knowledge is available in which Member State.

* **In the future, would you be willing to pay a fee to obtain the additional 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 publishes interesting information notes, reports and knowledge and expertise products.
- ENISA supports implemention of policy. For example ENISA's work as the Secretariat of the CSIRTs Network.
- ENISA's work in organizing Cyber Europe.

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

- Instead of publishing many reports ENISA should focus more on being a knowledge broker and make use of the knowledge and expertise that is available in the Member States and translate when necessary.
- In these reports ENISA should include clear authoritive policy recommendations, perspectives for action that reflect/answer questions that the EU DG's and MS have.
- Strengthening public private cooperation by enforcing the Permanent Stakeholder Group.
- Next to Cyber Europe, also explore which other forms of capacity building are beneficial.

* **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:

```
It's not desirable to have offices in two parts of a country, for efficiency,
costs reaons and the time it takes to travel to Heraklion. We therefore
prefer one office in Athens with perhaps a permanent representation (PermRep)
in Brussels.
```

* 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:

The added value of the EU is that all MS are capable to share information on cybersecurity issues. This should be further strengthened. Standards and certification is a matter that must be addressed on an EU/International level. Furthermore, skills development and training of professionals is an issue that all MSs are struggling with, therefore EU work is desirable.

* **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:

We believe that the cooperation, complementarity and alignment between the bodies should be improved. Mainly in order to avoid overlap and to be able to strenghten each others efforts.

* 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
- [ ] 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
- [x] 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:

Strenghtening public private cooperation in cybersecurity

Please elaborate on your answer on the top priorities:

- further strenghtening the Cooperation Group and the CSIRTs Network and existing bodies. (no duplication)
- A framework for security certification of IT products and services with an aim to create a level playing field in the EU (wording such as harmonisation should be avoided in this regard).
- Public private cooperation is essential in the field of cybersecurity and should be further stimulated.

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:

none

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

- Stronger cooperation within the existing networks.
- ENISA has a role in facilitating/supporting the cooperation amongst Member States, including operational cooperation. ENISA does not have an operational role itself.
- In order for ENISA to be able to support the Commission and Member States in implementation of directives for example, ENISA requires extensive knowledge. Also to be able to fuel to Commission with neutral advices.

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

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.

```
In addition:

- the focus of ENISA's work is shifted partly, therefore we believe it is
important to also take this into account when selecting and attracting new
staffmembers. The required competences should not only contain cybersecurity
skills but also diplomatic, policy and networking/accountmanagement skills.
- The CSIRTs Network is an important cooperation mechanism for EU operational
cooperation. ENISA supports this as the secretariat and hence should not have
any operational capacity.
- In the field of large scale cyber incident in the EU, the responsibility
lies first and foremost within the EU Member States. ENISA may have a
facilitating and supporting role in this.
```

Contact

CNECT-FEEDBACK-ENISA@EC.EUROPA.EU