Contribution ID: 30f30291-9904-4f1e-a9a0-d8f1e50d775c
Date: 04/04/2017 10:45:49

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:**

Jukka S.

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

Rannila

* **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”.

jukka.rannila@netikka.fi

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

Finland

* **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.)

* **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

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:

–

* **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

* 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:

–

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.

```
–
```

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.

38aaacd1-2795-4d33-aef4-1a0dfcbc05be/ENISA_review_2017_JUKKA_RANNILA.pdf

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

```
I added a PDF file my opinion.
```

Contact

CNECT-FEEDBACK-ENISA@EC.EUROPA.EU