European
Commission

# Evaluation of ENISA

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

A study prepared for the European Commission
DG Communications Networks, Content & Technology by:

CARSA RAMBOLL

*Digital Single Market*

**This summary report was developed as part of the evaluation of ENISA for the European Commission by**

Karin Attström, Vanessa Ludden, Franziska Lessmann
Ramboll
www.ramboll.com

Pär Weström, Johannes Conrads
Carretera de Asúa, 6
48930 Getxo
Vizcaya – España
http://www.carsa.es/en/index.php

**Internal identification**

Contract number: No 30-CE-0815229/00-33 implementing Framework contract No 30-CE-0677656/00-00

SMART number 2016/0077

**DISCLAIMER**

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-72111-3

doi:10.2759/964204

## CONTENTS

## FIGURES

# 1. INTRODUCTION

ENISA was set up in 2004 with the overall goal of ensuring a high level of network and information security within the EU. ENISA has since supported European institutions, Member States and the business community in addressing, responding to and preventing network and information security problems.

The open public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA) took place between 18 January and 12 April 2017. It was conducted in the context of the evaluation and review of ENISA in accordance with Article 32 of Regulation (EU) No 526/2013.

The open public consultation aimed to gather the views of stakeholders and interested parties to assess ENISA's overall contribution to the cybersecurity landscape for the period 2013 to 2016. The public consultation will also contribute to a reflection on potential policy options for the revision of ENISA's mandate. For this purpose, the consultation was structured around two sections:

- Backward looking – ex-post evaluation of ENISA
- Forward looking – focusing on evolving needs and challenges in the cybersecurity landscape and the possible role of an EU body to meet them in the future

Respondents were allowed to respond to either one or both sections. In addition, respondents had the possibility to send position papers. These papers have been considered for the qualitative analysis, but not in the statistical representation.

This synopsis report takes stock of the contributions received and presents the trends that have emerged from the qualitative and quantitative analysis of the responses.

In addition to presenting overall results, this report categorises the responses received according to the following three stakeholder groups:

**Table 1: Categorisation of stakeholder responses**

| 1. National authorities | 2. Private enterprises and business associations | 3. Other |
|---|---|---|
| • **National authorities** | • Private enterprises<br>• Trade business or professional association | • Individual respondents<br>• Non-governmental organisations (NGOs), platform or network<br>• Professional consultancy, law firm, self-employed consultant<br>• Research and academia<br>• Other |

*<u>Disclaimer</u>: With a total of 90 responses, the results of the open public consultation cannot be considered to be fully representative of all stakeholders concerned. However, the views of national authorities of 15 Member States (including the position paper provided by France) are represented. The private sector is represented by 27 respondents which include eight umbrella organisations, thus representing a significant number of European enterprises whose activities are linked with cybersecurity.*

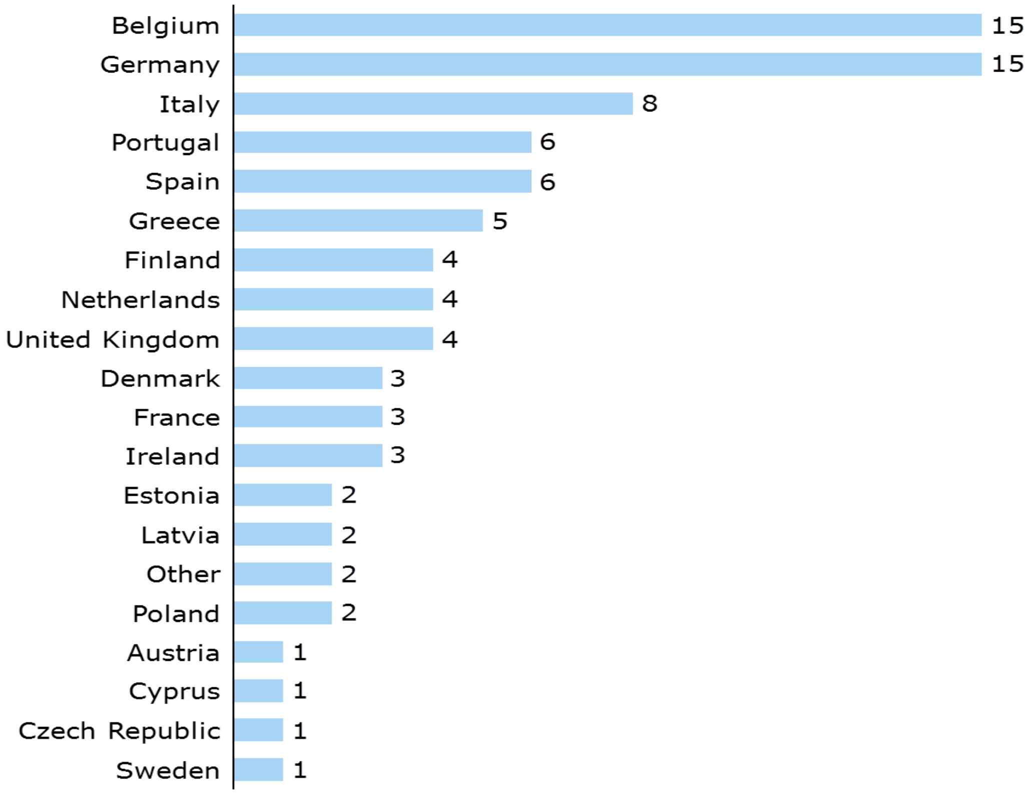
## 2. RESPONDENTS' PROFILES

In total, 90 responses to the open public consultation were received, out of which 88 consisted of responses to the questionnaire. Two position papers were received as part of the consultation process and a further two respondents provided written contributions together with their response to the consultation questionnaire.

The two position papers provided were from the public authorities in France and a business association from the United Kingdom. These have been taken into account in the analysis of the qualitative contributions to this consultation and in the findings and conclusions for the overarching evaluation of ENISA.

Respondents from 19 different Member States participated in the open public consultation.

**Figure 1: Country of residence of respondents (N=88)**



The two respondents that indicated a country of residence outside the EU were from Switzerland and the United States.

*The responses are shown in percentages with absolute numbers in brackets throughout the summary report.*

**More than half of the respondents (45 out of 88) to the consultation questionnaire answered on behalf of an organisation**, while just over a quarter answered in their professional capacity (23) and almost a quarter of respondents (20) answered in their personal capacity.

The largest proportion of the respondents that answered on behalf of an organisation represented the private sector (22) which included private enterprises and representative business associations. Respondents representing national authorities were the highest respondent group (14).

*Note, however, that members of the CSIRT Network (28 EU Member States + CERT-EU) were also consulted through a dedicated survey as part of the overarching evaluation of ENISA.*

### Table 2: Type of organisation of respondents answering on behalf of an organisation (n=45)

| Types of Organisations | % of respondents answering on behalf of an organisation | Number of respondents<br>n=45 |
|---|---|---|
| National authority | 31% | 14 |
| Private enterprise | 31% | 14 |
| Trade, business or professional association | 18% | 8 |
| Non-governmental organisation, platform or network | 13% | 6 |
| Research & academia | 4% | 2 |
| Other | 2% | 1 |

With regard to contributions from respondents answering in their professional capacity, a total of 23 responses were received. These were mostly researchers or academics, professional consultants or employees of private enterprises.

**Among those who answered either on behalf of an organisation or in their individual professional capacity (68 respondents in total), the largest proportion (30) worked in the field of cybersecurity** while the rest primarily worked in telecommunications (11) and "other" sectors (11) focusing on advisory & research and government affairs.

A total of 17% of respondents (15) to the open public consultation belonged to ENISA's Executive Board, Management Board, Permanent Stakeholder Group (PSG) or the National Liaison Officers (NLOs).

69% of respondents (61) answered both the retrospective and forward looking questions; 26% (23) contributed solely to the assessment of ENISA's future and 5% (4) solely to the questions relating to ENISA's activities over the 2013-2016 period.

# 3. RESULTS

## 3.1 Backward looking questions

The following section of the questionnaire has been used to provide information on the evaluation criteria relevance, effectiveness, coherence and added value of ENISA. It presents participants' assessment of ENISA's overall contribution to Network and Information Security (NIS) in the EU during the 2013-2016 period.

**Main trends:**
The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%) as contributing to network and information security in the EU. A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each individual objective).

In general, ENISA's work was considered to be coherent with the work of other entities, including other EU agencies and bodies (68%).

ENISA's services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).

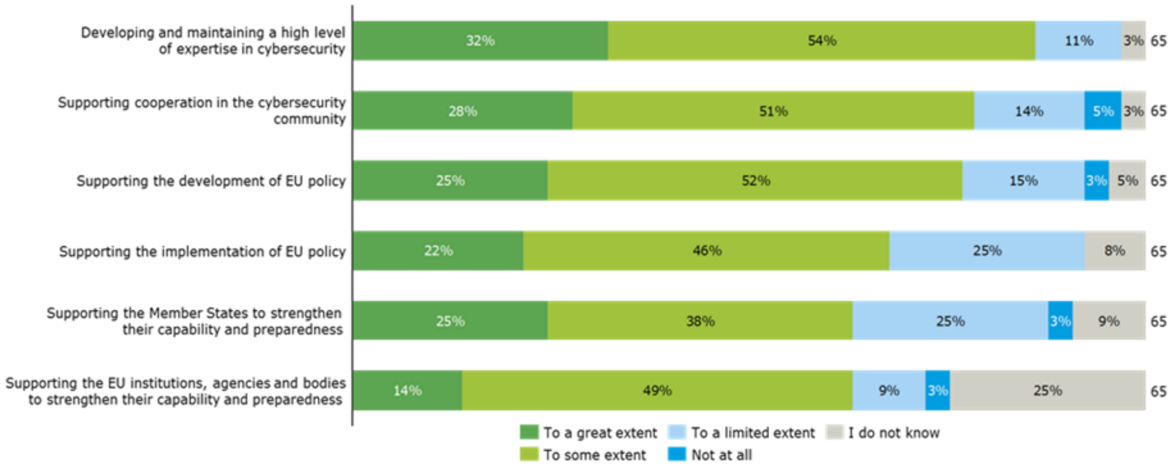
A majority of respondents considered ENISA's size in terms of staff members to be insufficient (59%).

### 3.1.1 ENISA's contribution to network and information security in the EU

All 65 respondents indicated that ENISA had achieved its objectives, as **set out in its mandate**, to some or to a great extent.

The assessment made by the respondents is presented in Figure 2 below.

### Figure 2: To what extent has ENISA achieved the following objectives over 2013-2016? (n=65)



When comparing the responses of different stakeholder categories, it appears that each category of respondents identified the objective of their interest as where ENISA's performed the best:

- All national authorities stated that "Supporting the implementation of EU policy" had been achieved "to a great extent" or "to some extent"
- Private enterprises or business associations most frequently (71%) indicated that ENISA had achieved "Supporting cooperation in the cybersecurity community e.g. though private-public cooperation, information sharing, enhancing community building"
- "Other" respondents most frequently (85%) indicated that ENISA had achieved "Developing and maintaining a high-level of expertise in cybersecurity"

Additionally, a majority of respondents agreed on all objectives that they had been met at least to "some extent".

Respondents were asked to comment on what they perceived as **ENISA's main achievements over 2013-2016**. Respondents across all groups cited the following as ENISA's main achievements:

- The coordination of the Cyber Europe exercises
- The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange
- ENISA's publications as support to the drafting and reviewing of national security frameworks, as well as reference document to policy makers and cyber practitioners
- Assisting with the promotion of the NIS Directive
- Efforts to increase awareness on cybersecurity via the yearly European cybersecurity month

*National authority respondents* added as a main achievement the support that ENISA provided to Member States, for examples: sharing of expertise among Member States, information sharing on Article 13[1], and support for the eIDAs[2] implementation.

[1] Art. 13a, of Directive 2009/140

[2] Regulation (EU) No 910/2014

P*rivate enterprises and business associations* for their part commended ENISA's work in fostering public-private cooperation and increasing better cross-sector engagement. One of the respondents noted that ENISA provides a degree of "coordination and harmonisation that might have otherwise been missing". ENISA was also seen as a neutral source of relevant information. Respondents described ENISA as a source of knowledge that is easily accessible and easy to use, covering a wide range of cybersecurity topics.

Respondents were then asked to comment on the **areas where they considered ENISA could have done better** over the period of 2013-2016. The 52 open responses received can be grouped into four themes:

With regard to its *publications*, according to national authorities, private enterprises and business associations ENISA could have done better by:

- Covering fewer topics with the needed depth, focusing more on being a knowledge broker through the use of knowledge and expertise available in Member States
- Providing publications with a more global scope

With regard to its *involvement in policy & guidelines*, according to private enterprises and business associations ENISA could have done better by:

- Proposing common criteria to assess and manage cybersecurity risks/ harmonised threat-informed risk-based approach
- Proposing technical solutions to the most common attacks
- Improving its yearly report on the threat landscape with a clearer indication of what has changed and showing awareness of the top current attacks
- Coordinating consistent dialogue with Member States on the implementation of the NIS Directive[3]

As for national authorities, they suggested that ENISA could have provided clearer policy recommendations and simplified guidelines for more effective communication.

With regard to its *involvement in stakeholder cooperation*, national authorities suggested that ENISA could have done better by:

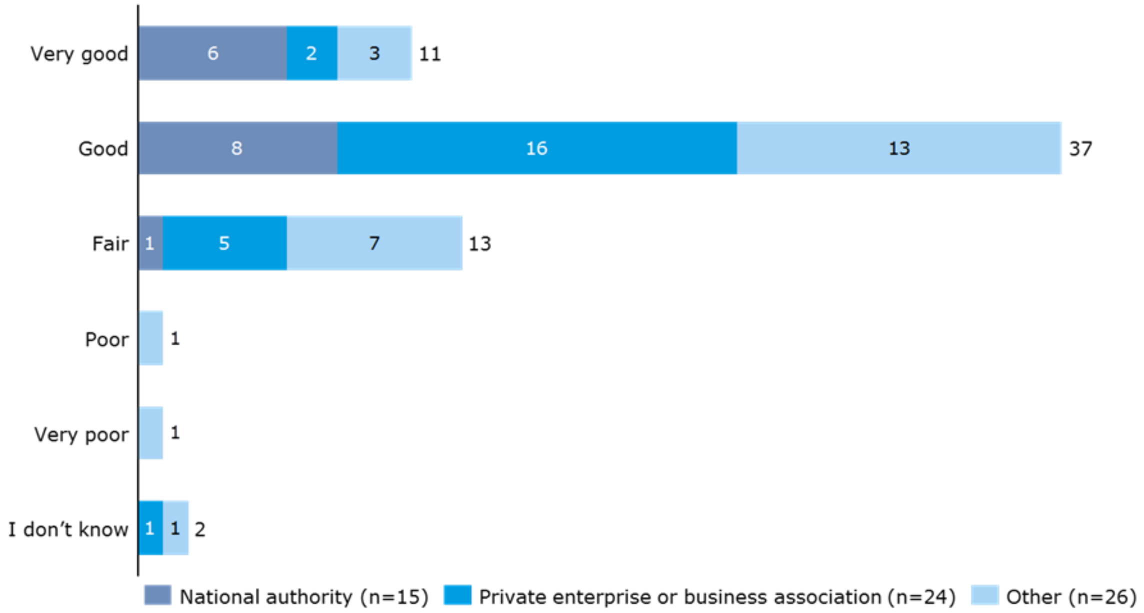
- Enhanced collaboration with Member States
- Making greater efforts to raise awareness on cybersecurity by collaborating with other EU organisations
- Playing a more central role in other EU cybersecurity initiatives such as Cyber Public-Private Partnership (cPPP) or the European Cyber Security Organisations (ECSO) from the beginning
- Avoiding overlap with the work of standardisation bodies and focussing its operations on areas not covered by the tasks of national authorities
- Improving the involvement of national experts and competent authorities in its working groups

Private stakeholders also suggested that ENISA could have been more involved in fostering public-private partnerships. Moreover, they suggested that ENISA should have consulted with a greater range of stakeholder groups on work priority to allow all of them to provide feedback.

[3] Directive (EU) 2016/1148

Finally, respondents were asked to give an **overall assessment of ENISA for the period of 2013-2016**. Overall, 74% of respondents (48) had a positive view of ENISA. Most national authority respondents assessed ENISA for the period of 2013-2016 as “good” to “very good”, while private enterprises and “other” respondents mainly assessed it as “good” to “fair”.

**Figure 3: To conclude this section, please give your overall assessment of ENISA for the period 2013-**



### 3.1.2 Coherence of ENISA’s activities with those of other organisations

83% of respondents considered ENISA’s activities to be to a “large extent” or to “some extent” **coherent with** (i.e. take into account, do not overlap, do not conflict with) **the policies and activities of their own organisation**.

When asked about **coherence with other organisations, including other EU agencies and bodies**, 68% of respondents (44) considered ENISA’s activities to be to a “large extent” or to “some extent” coherent.

Respondents who evaluated ENISA’s activities as “somewhat, but to a small extent” or “no, not at all” coherent pointed to a general lack of coherence in the EU’s approach to cybersecurity. More specifically, concerns were raised with regard to the delineation of competences between ENISA and other EU agencies, most importantly CERT-EU.

It is worthy of note that a significant proportion of respondents were unable to express a view on this topic.

### 3.1.3 Interaction with ENISA

Nearly half of respondents (46%) interact regularly, i.e. at least once a month, with ENISA’s products and services.

The **top products or services used by respondents** were as follows:

- the Guidelines & recommendations, including on standards (cited by 90% of respondents)
- the Reports (e.g. NIS Threats Landscape) & Research Publications (cited by 85%)

Respondents were asked to select out of a list of eight options their **reasons for using ENISA's products and/or services**. The most frequent reasons given were:

- The products and services are provided by an EU-level body (stated by 83% of respondents)
- The products and services are free of charge (stated by 67%)
- The products and services can be trusted (stated by 63%)

Respondents were asked to consider **to what extent ENISA's products and services over 2013-2016 had responded to the emerging needs of the cybersecurity community in a timely manner**; 87% of respondents (54) said they had "to a large extent" or "to some extent". This was a consistent assessment across all respondent categories.

Asked **if there were any other products or services they would have liked ENISA to provide** the cybersecurity community with over 2013-2016 35% of respondents, largely from the private' sector, answered "yes". What those respondents were missing can be categorised in four broad topic areas, namely:

- providing operational capacities (providing incident information),
- developing enhanced cross-country cooperation across Member States and but also with non-EU countries
- providing additional policy & guidelines (e.g. providing benchmarks to the private sector)
- providing support for innovation (e.g. for start-ups in the area of cybersecurity) .

### 3.1.4 Location and organisational structure

Respondents were asked **whether** they felt that **ENISA's split location between Heraklion and Athens affected its ability to conduct its work effectively and efficiently**. There were mixed perceptions expressed in relation to this question with 28% (18) judging that the split location affected ENISA's ability to conduct its work effectively and efficiently to "some extent" or to "a large extent", while 20% (13) stated it did "not at all".

Lastly, respondents were asked to consider the **current size of the Agency**, with 84 staff members, and assess whether this was adequate for the work entrusted to ENISA. 58% of respondents (38) considered the size of the Agency to be partially or completely inadequate. There were no notable differences between the different respondent groups.

## 3.2 Forward looking questions

The subsequent section presents respondents' assessments of what the needs and gaps in the cybersecurity landscape are in Europe from today's perspective. The questions in this section are intended to look ahead to the next ten years.

**Main trends:**
Overall, respondents identified a number of gaps and challenges for the future of cybersecurity in the EU and a large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these.

Enhanced cooperation between Member States and between the public and private sector, as well as further research and sharing of knowledge were judged to be the main needs for the coming years.

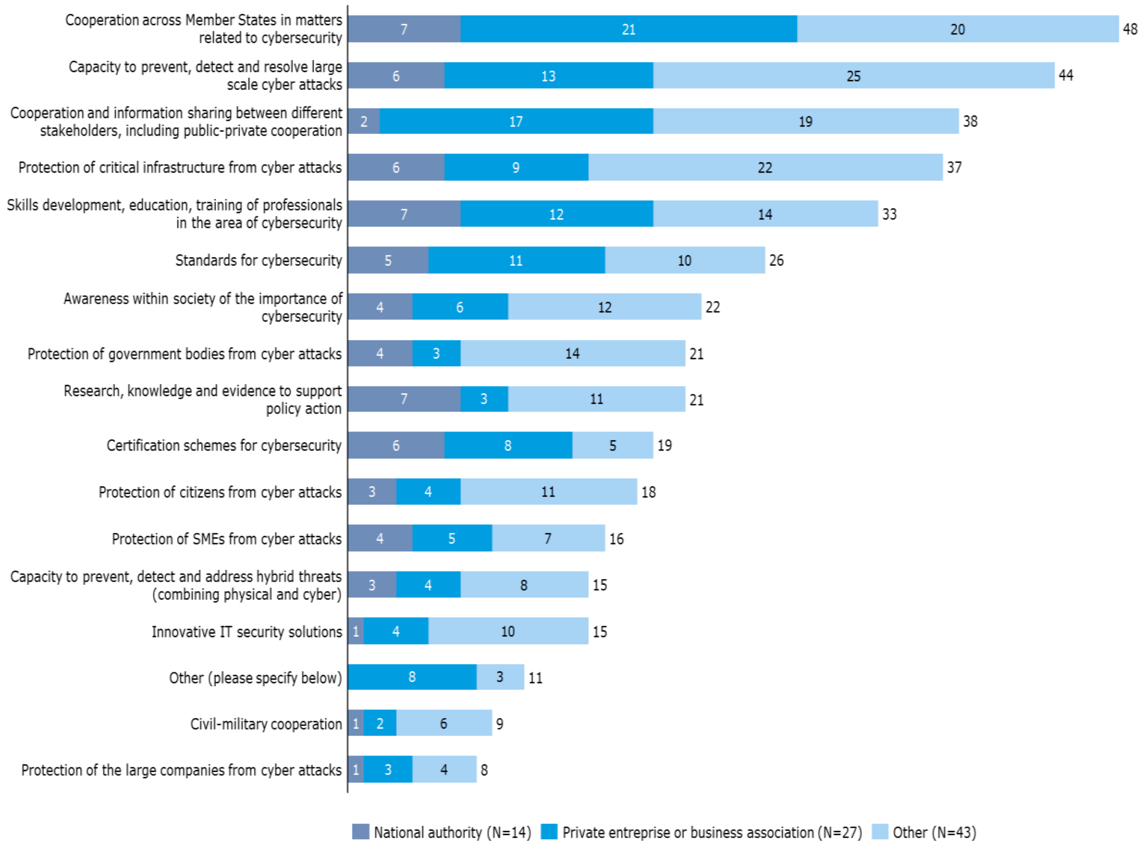
A large majority of respondents (98%) saw a need for an EU body to respond to these needs and of all EU bodies ENISA was considered to be the right organisation to do so by 99%. Generally, ENISA was judged to be capable of responding to the various needs and gaps identified.

### 3.2.1 Future needs and challenges

In relation to the evolving cybersecurity landscape and the current EU policy response, respondents were asked to select **the most urgent needs or gaps in the cyber security field in the EU** over the next ten years among a list of 16. From the assessment made by 84 respondents, the largest number of respondents identified "Cooperation across Member States in matters related to cyber security" and the "Capacity to prevent, detect and resolve large scale cyber-attacks" as a main gap or need in the cybersecurity field in the EU over the next ten years.

As Figure 4 shows, the views of the different respondent groups in relation to each of the options were relatively balanced.

### Figure 4: What will be the most urgent needs or gaps in the cybersecurity field in the EU in the next ten years? Please select up to 5 options (n=84)



13% of respondents stated that there are **other urgent needs or gaps** in the cybersecurity field in the EU in the next ten years, these included:

- Capacity to prevent, detect and resolve cyber-attacks including industrial espionage
- Coordination between EU cyber-agencies and private sector
- International cooperation (i.e. EU and third countries such as the US, Japan, Korea, India)
- Fundamental research to further advance security of complex systems by design
- Technologies for the protection of privacy
- Protection of electoral processes and political parties

Respondents were asked to **elaborate further**; 55 did. Their answers are summarised below:

- As for the *need for increased cooperation* across Member States respondents suggested that cooperation was necessary not only to bridge the security gaps that arise from a lack of cross-country cooperation, but also to build trust and confidence within the EU. Some respondents pointed to additional benefits of such cooperation, including increased market integration through the provision of internet services, support to the increase in cybersecurity capacity of less advanced Member States, and innovation for responses to current and future threats.
- As for the *needs for harmonised standards and certification in the field of cybersecurity*, respondents stated that the establishment of a common certification framework would help bridge inconsistencies and gaps in the implementation of security controls as well as to achieve trust across Europe. The achievement of this closely depended on coordination at Member State level.
- As for the *need to increase capacity to prevent, detect and resolve attacks* respondents pointed to the fact that the EU should step up the detection and real-

time response to cyberattacks in information, communication technology (ICT), critical infrastructures, SMEs, government and public agencies. Others felt that the priority should rather be placed on developing a prevention-focused approach that allows protection from loss of intellectual property and personal data as well as loss of trust.

- As for *skills development and education in the field of cybersecurity*, respondents saw the need to adapt the skills for cybersecurity professionals much closer to the evolution of the needs of the market needs. Respondents further commented that increasing citizen awareness on the importance of cybersecurity was a necessary gap to be filled given that "the human element is the weakest".

In this context, respondents from the groups of private enterprises and business associations and "other" respondents proposed a set of roles that ENISA could take on to address the identified needs or gaps, these included:

- ENISA taking on a more proactive role in coordination of EU institutions, Member States and the private sector, facilitating cooperation and effective flow of threat and incident information for swift responses and adaptation of security defence solutions
- ENISA taking on a role in supporting research in cybersecurity in the form of public-private partnerships
- ENISA supporting the harmonisation of standards and certification by promoting existing internationally agreed standards and frameworks
- ENISA supporting government efforts on the development of a cybersecurity workforce through the development of guidelines
- ENISA playing a role in ensuring that national transpositions of the NIS Directive are homogeneous

Respondents were asked to consider **if the current instruments and mechanisms at European level are adequate to promote and ensure cybersecurity with respect to the needs previously identified**. Only 6% of the consultation respondents judged the current instruments and mechanisms at European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be "fully adequate" to promote and ensure cybersecurity. 83% of respondents regarded them as either "partially" or only "marginally adequate". National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms than the rest of the respondents.

Respondents who assessed the current instruments and mechanisms as "partially adequate", "marginally adequate" or "not at all adequate" were asked to elaborate on their responses and 51 did, providing further assessments and recommendations for improvement:

- Respondents positively assessed the progress the EU has made in the set-up of its regulatory and institutional framework for cybersecurity. However, they also stated that the majority of the instruments had yet to be implemented, enter into force or still needed to be developed. Three respondents stated that the framework is too often open to interpretation, which "leaves the possibility of non-harmonised implementations" that are contrary to its aim.
- Respondents further noted that the NIS Directive has not fully addressed the needs, challenges and threats faced by all affected industries. The differences in threats and financial constrains across industries should be born in mind. It was also suggested that the cooperation mechanisms created by the NIS Directive should be evaluated after two years.
- A few "other" respondents commented that the development of standardisation and certification regarding information security at EU level should be improved

and accelerated. As an example, on IT solutions respondents felt Internet-of-Things-risks ought to be addressed more strongly and EU-made cybersecurity solutions developed by the private industry (SMEs) should be supported.
- Respondents found existing cooperation mechanisms insufficient to address upcoming challenges and threats and to achieve convergence in standards for protection. Specifically the lack of mechanisms that could enable information sharing or collaboration between the EU and third countries.

Based on the identified needs or gaps, consultation respondents were asked to **consider what the priorities for EU action should be from now on** and select up to three responses out of a list of 15. "Stronger EU cooperation mechanisms between Member States, including at operational level" was most frequently selected as a top priority, followed by "Stronger public-private cooperation in cybersecurity" and "improving research to address cybersecurity challenges".

The 12 respondents who selected "other" in response to this question were asked to further specify additional top priorities for EU action:

- Six of the priorities mentioned related to *cooperation*. Besides pushing for "stronger public-private cooperation", respondents pointed to "establishing stronger international / trans-Atlantic cooperation and collaboration" including regulatory convergence, as well as "developing policy and operational support for cooperation and information sharing between different stakeholders and Member States".
- Five other priorities concerned *support and guidance* in areas such as "support in the uptake of new privacy techniques", "improved monitoring of threats", "Provision of implementation, application and enforcement tools" and an "EU-reviewed open source, for public administration i.e. communes".
- Finally, three other identified priorities related to *cybersecurity regulation* where respondents asked for "more flexibility in regulation to allow adapting to the nature of organisations, services and markets" and believed that ENISA's role with regard to this should be to "sign-post relevant and robust standards that function at global level" given its "important role in harmonisation across the EU".

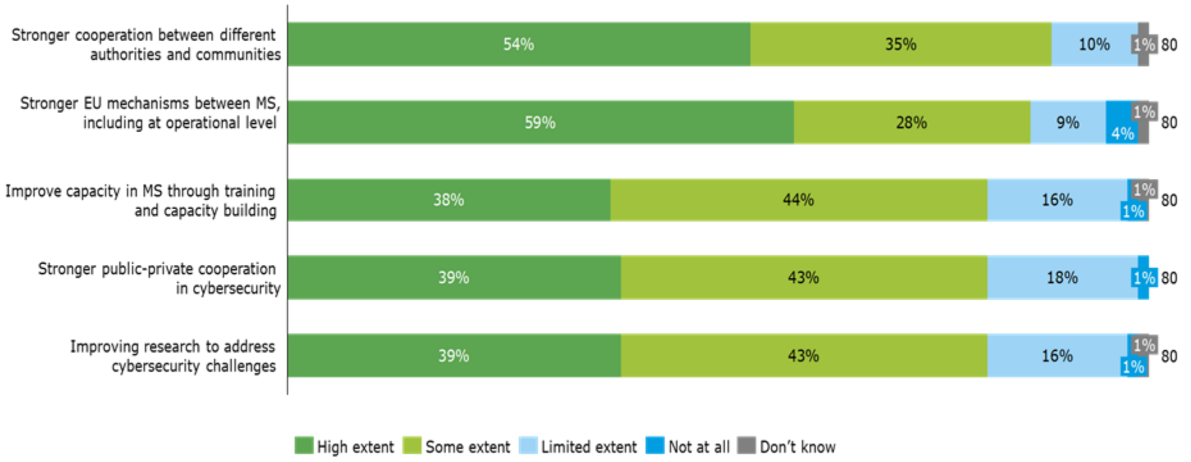
### 3.2.2 The role of an EU body in the future EU cybersecurity landscape

98% of respondents (82) saw a **role for an EU-level-body in improving cybersecurity across the EU**.

Furthermore, 81 out of the 82 respondents considered that **ENISA could fulfil a role in bridging the different gaps in the future**.

The Agency, if sufficiently mandated and resourced, was perceived as **most able to fulfil the five roles as below.**

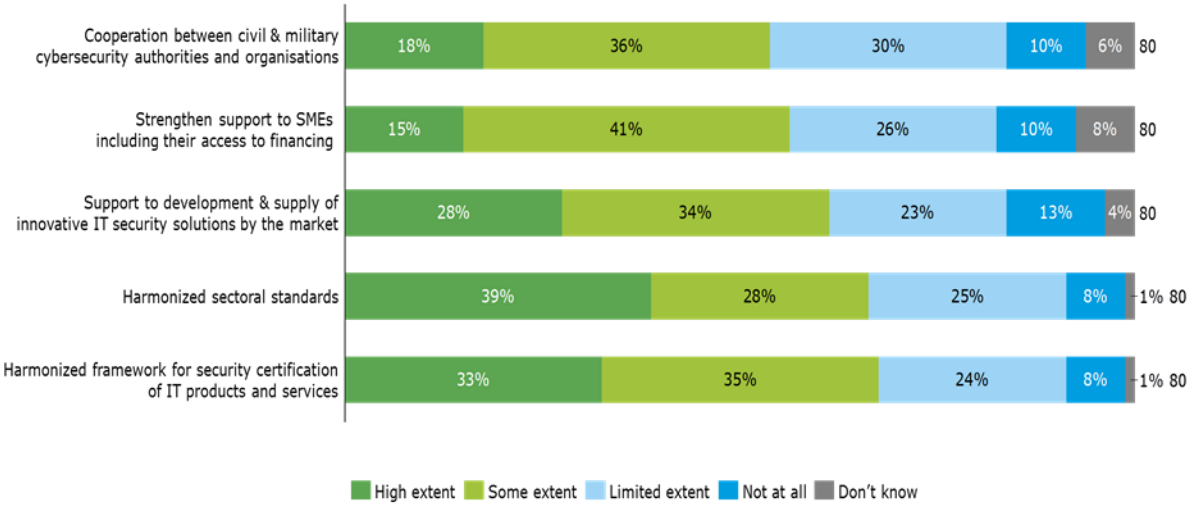
### Figure 5: Five roles where, if sufficiently mandated and resourced in the future, ENISA could bridge the gaps identified to the highest extent



On the other hand, the Agency was perceived as **least able to contribute to the following five areas** (

Figure 6 below presents the specific roles which most respondents considered ENISA to be able to fulfil to "a limited extent" or "not at all"):

### Figure 6: Five roles where even if sufficiently mandated and resourced in the future, ENISA would be able to bridge the gaps identified to a lesser extent



In summary, respondents to the open public consultation consider ENISA to be the right body to respond to the needs they identified as most pressing. However, a more detailed analysis of the answers indicates clear differences in opinion per type of respondent group in some areas. In this sense "Stronger cooperation between different authorities and communities" was less supported as a role for ENISA by national authorities compared to the other respondents. Conversely, "Stronger public-private cooperation in cybersecurity" received higher support from private enterprise and business association respondents.

Bearing in mind the previous assessments on the gaps and needs in the cybersecurity landscape, respondents were asked to provide **examples of what ENISA's future**

**role could be in addressing these gaps and needs**, if they deemed it had one. The role seen for ENISA covered the following activities: fostering cooperation between Member States at international level and between the public and private sector; having a stronger role in policy development and implementation; ensuring harmonisation of approaches and setting baselines; certification and standardisation; providing incident response information; ensuring awareness raising, training and capacity building; supporting the private sector; ensuring the transposition of the NIS Directive; and fostering research.

National authorities expressed stronger views on ENISA 's future role than the other respondents: Three national authorities underlined that ENISA should not take on an operational role in providing incident response activities, in view of potential overlaps with CERT-EU and the need for the Agency to focus its resources on its core activities. Respondents stressed that the future role of ENISA relied on sufficient human and financial resources and a clearer division of responsibilities between the different EU institutions and bodies active in the area of cybersecurity, most importantly CERT-EU.

Almost all respondents agreed that there is a future role for ENISA in addressing the gaps and needs identified.

While respondents to the open public consultation pointed to **other EU initiatives to help respond to current gaps and needs**, these were not seen as alternatives to ENISA. Consultation respondents were asked to propose what other, if any, EU initiatives could be put in place to address the gaps and needs identified. In total, 38 respondents commented:

- *National authority respondents* stated that other EU initiatives could focus on "increased funding for capacity building and joint operational ventures, particularly for smaller Member States" and "further financial programmes to support CSIRTs capabilities and SMEs protection". For this, ENISA should be allowed to participate in funding programmes to ensure more effective work with Member States and to extend the range of activities it offers.
- National authorities also stated that initiatives should target the harmonisation of legislation across EU Member States aiming at creating more adequate and harmonised standards and authorities "with a clear cooperation and information sharing framework between them".
- *Respondents from private enterprises and business associations* commented on various topics: Specifically on the NIS Directive, a few respondents felt the current legislation was already outdated before the implementation process could be completed; therefore a revision of the Directive was considered necessary. Other contributions showed strong support for the EU to invest more in addressing the cyber skills gap.
- *Respondents from the "other" stakeholder group* agreed that there must be a better approach to legislation, particularly due to the "slightly chaotic process surrounding the launch and subsequent debate on the NIS Directive". Additional laws were not seen as necessary, but rather "effective continuous action" by focusing on education and information sharing at a fast pace. Other respondents also saw the need for the "establishment of a dedicated funding or financial programme for cybersecurity research", suggesting it would be a "powerful incentive for government, universities and the private sector to help archive security goals".

European Commission

**Evaluation of ENISA - Public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA) - ANNEX**

Luxembourg, Publications Office of the European Union

**2017 – 18 pages**

ISBN 978-92-79-72111-3
doi:10.2759/964204

KK-04-17-748-EN-N

doi:10.2759/964204

ISBN 978-92-79-72111-3