European
Commission

Study on the Evaluation of the European Union Agency for Network and Information Security

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

RAMBØLL

carsa

Digital Single Market

This study was carried out for the European Commission by

Karin Attström, Vanessa Ludden, Franziska Lessmann
Ramboll

Pär Weström, Johannes Conrads
Carsa
Carretera de Asúa, 6
48930 Getxo
Vizcaya – Spain
http://www.carsa.es

With contributions from Helena Farrand Carrapico, Aston University; Andrej Savin, Copenhagen Business School; Cristina de la Maza, RedBorder

Internal identification

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

SMART 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 978-92-79-72114-4
doi:10.2759/94930

ABSTRACT

The European Union Agency for Network and Information Security (ENISA) was established in 2004. The Agency provides advice and recommendations, data analysis, and supports awareness raising and cooperation by the EU bodies and Member States in the field of cybersecurity. ENISA uses its expertise to improve cooperation between Member States, and between actors from the public and private sectors, as well as to support capacity building.

The present study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency's performance, governance and organisational structure, and positioning with respect to other EU and national bodies. It assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It also provides options to modify the mandate of the Agency to better respond to new, emerging needs and assesses their financial implications.

The findings of the evaluation study show that ENISA has made some important achievements towards increasing NIS in the EU. However, a fragmented approach to cybersecurity across the EU and issues internal to the Agency, including limited financial resources, hinder ENISA's ability to respond to the ever growing needs of stakeholders in a context of technological developments and evolving cybersecurity threats.

EXECUTIVE SUMMARY

This is the executive summary to the "Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA)".

Objectives

ENISA is the EU agency for network and information security. It was established in 2004 by Regulation (EC) No 460/2004. Since then, ENISA's mandate has been reviewed once and the Agency's mandate has been extended several times. The latest changes were implemented with Regulation (EU) No 526/2013 (hereafter "the Regulation"). Article 32 (1) of the Regulation requires the Commission to "commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency ad its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification".

The study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency's performance, governance and organisation structure, and positioning with respect to other EU and national bodies. Furthermore, the study assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It provides options to modify the mandate of the Agency to better respond to the new needs and assesses their financial implications.

Methodological approach

The evaluation study aims to assess the relevance, effectiveness, efficiency, coherence and complementarity, and EU added value of ENISA. It contains responses to 46 evaluation questions based on the European Commission's Roadmap for the evaluation of ENISA[1]. The evaluation conclusions are drawn from both primary and secondary data collection and analytical tasks which feed into the development of the answers to the evaluation questions. The evaluation involved extensive data collection, including the consultation of various stakeholders groups (such as ENISA staff and management, ENISA's Management Board, national Computer Emergency Response Teams and Computer Security Incident Response Teams (CERTs/CSIRTs), EU institutions, private stakeholders). Primary data was collected through different tools: in-depth interviews, two surveys, an open public consultation and a workshop. The evaluation is underpinned by an evaluation matrix, which links the evaluation questions to the data sources, indicators and analytical strategies that were used to answer them, thus making it clear how the conclusions have been reached.

The evaluation was carried out between November 2016 and July 2017 by Ramboll Management Consulting and CARSA, and involved three external experts covering the policy, legal and technical aspects of cybersecurity.

Findings and conclusions

An assessment of ENISA's performance, governance and operational structure and positioning for the period 2013-2016 according to the evaluation criteria is presented in the following table. The key findings that have led to this assessment are presented below.

Table 1: Assessment of ENISA against the evaluation criteria

Evaluation criterion	Overall assessment
Relevance	Achieved to a large extent
Effectiveness	Partially achieved
Efficiency	Achieved to a large extent
Coherence	Partially achieved
EU-added value	Partially achieved

[1] European Commission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA)

Relevance: In the context of technological developments and evolving threats, there is a significant need for increased network and information security (NIS) in the EU. The recent additions to the legislative framework, such as the NIS Directive[2] underline this. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Considering this context, the objectives set out in ENISA's mandate proved to be relevant over the period under evaluation and continue to be of high relevance today.

While the mandate defines the Agency's objectives in broad terms, leaving room for ENISA's Management Board to set priorities based on latest developments in order to respond to changing needs and evolving threats, ENISA's activities do not fully meet the needs of all its stakeholders:

- ENISA's work programme is dominated by the interests of the Member States, and yet it is necessary to consider the longer-term perspective and the activities of other stakeholders in the cybersecurity area (such as other EU agencies or the private sector) to ensure continued relevance of the Agency
- ENISA's stakeholders strongly differ in their needs, making it difficult to meet them all. Some Member States (such as Germany, France or Sweden) have significant capacity and resources in the area of cybersecurity and rely on ENISA only for specific services. Other Member States (from Eastern and Southern Europe) are less experienced and rely more strongly on the expertise and capacity of ENISA. The Commission has their own needs and expectations with regard to the services that ENISA can provide to the different DGs. Additionally, industry stakeholders, including a high number of Small and Medium Enterprises (SMEs) are important actors in NIS and could also benefit from ENISA's activities

Effectiveness: In general, ENISA implements its tasks and achieves its set targets. ENISA has made a contribution to increased NIS in Europe through the four tasks presented in the table below, though there is room for improvement in relation to each.

Community building		**Capacity building**	
Achievements	Areas for improvement	Achievements	Areas for improvement
✓ Important contribution to enhanced cooperation between Member States and related NIS stakeholders, in particular between CERTs/CSIRTs	- Cooperation could be strengthened between ENISA and the Commission and other EU agencies, and with the private sector	✓ Contribution to enhanced capacities in the Member States, most notably in Member States with limited capabilities and resources in the area of cybersecurity ✓ Important activities include the Cyber Europe Exercises and trainings for CERTs/CSIRTs	- Capacity building with the private sector could be increased

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Expertise provision		Supporting development and implementation of policies	
Achievements	Areas for improvement	Achievements	Areas for improvement
✓ Important contribution by supporting CERTs/CSIRTs	- ENISA has not managed to become recognised as a centre of expertise or a reference point for other stakeholders, such as EU institutions or the private sector - High reliance on procurement of external expertise and limited resources available in-house	✓ ENISA has assisted the Member States and the Commission in developing and implementing policies	- ENISA is not consistently being involved by the Commission in all NIS-related activities

ENISA's contribution to NIS in Europe is limited by several key factors, including:

- The broad mandate under which a variety of tasks is to be covered, leaving limited scope to work on its own initiative and other than upon request
- The Agency's difficulties in attracting and retaining cybersecurity experts as staff members, due to various reasons including weak human resources procedures during the period under review
- The limited visibility of ENISA – the Agency is not sufficiently known across the EU and has not been able to establish a brand, unlike other EU agencies

Efficiency: ENISA has among the lowest budgets and levels of human resources compared to other EU agencies. In order to complete the various tasks set out in its mandate, ENISA has to be very efficient in the implementation of its budget and carefully consider where resources and working hours can be spent. The Agency develops a high number of publications every year and implements many other activities. Despite its small budget, the Agency has been able to contribute to targeted objectives and impacts, showing efficiency in the use of its budget.

In terms of efficiency, ENISA faces two main challenges:

- A number of administrative requirements set by the Commission which are the same for all EU agencies but weigh more heavily on smaller agencies
- A location split between Athens and Heraklion, requiring additional efforts of coordination and generating additional costs

Coherence: ENISA's activities are generally coherent with the policies and activities of its stakeholders, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and the European Commission, as well as other EU bodies, is not fully utilised. For example, the division of responsibilities between ENISA and CERT-EU should be clarified.

ENISA's activities are largely coherent with the work done at national level in the area of cybersecurity. Coherence is particularly strong between the CERTs/CSIRTs and ENISA. Some overlaps between ENISA's activities and those of Member States with strong cybersecurity expertise were identified, but Member States with less capacity and resources in the area of cybersecurity still benefit from its activities.

EU-added value: ENISA's added value lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value of ENISA differs between Member States, depending on their cybersecurity capacities and resources. The Agency's activities of providing expertise and capacity building represent important added value for Member States with few national resources dedicated to cybersecurity. This is less the case for Member States with more cybersecurity capacities.

Consequently, a discontinuation of ENISA would impact Member States differently. While Member States with strong cybersecurity capacities will be able to replace the services provided by ENISA at least to some extent, this will not be the case for Member States with fewer resources. The latter Member States rely more on ENISA's services in terms of capacity building, access to expertise and support in the implementation of policy and legislation. Cybersecurity crosses borders, so there is a need to build capacity to avoid weaker links that can impact on cybersecurity in the EU as a whole, as well as a need to provide a cross-EU response. It will not be possible to ensure the same degree of community building and cooperation across the Member States without a decentralised EU agency for cybersecurity; the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA. Therefore, coordination at EU level is needed.

A potential discontinuation of ENISA would be a lost opportunity for all Member States. Most stakeholders were of the opinion that ENISA could take on a more important role in the EU cybersecurity landscape in the future, ensuring a common response capacity. This potential for the Agency to capitalise on future opportunities would be lost should it be discontinued.

SWOT analysis: Based on an analysis of the context – namely the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape - the evaluation study provides an assessment of the main strengths and weaknesses of ENISA, and the opportunities and threats in the new cybersecurity and digital privacy landscape. These are presented in the figure below.

Table 2: ENISA's SWOTs

Strengths	**Weaknesses**
- Neutral, facilitator, free of political bias or commercial interests - Recognised support to Member States in capacity building & capability development to strengthen resilience to cyber-threats - Acknowledged collaboration & community building reaching wide range of actors, incl. Member States, industry, EU bodies etc. - Horizontal expertise, "landscape overview" of Member States cybersecurity policies	- Low visibility for various reasons: lack of expertise, weak communication/marketing and limited self-assertion within the EU cybersecurity policy landscape - Lack of a long-term, strategic vision - Recruitment difficulties - Reduced efficiency due to split location - Distance to EU decision makers in Brussels - Lack of financial and human resources to make a difference
Opportunities	**Threats**
- Growing need for synergies between information and communication technology (ICT) operators to ensure concerted and collaborative NIS policy actions - NIS Directive bears the potential to strengthen ENISA's role in EU cybersecurity policy - There is an acknowledged need and demand of stakeholders to strengthen awareness raising of cybersecurity - Stronger support in the community is evolving for ICT standardisation and certification	- Policy fragmentation at EU level and diverging policy priorities in EU Member States constrain ENISA's scope of action - Rapidly evolving and complex threat landscape involving multiple disciplines create new vulnerabilities, e.g. Internet of Things (IoT) - Lack of overall (technical) talent in the field of cybersecurity aggravates ENISA's recruitment difficulties

In conclusion, the following **key issues** have been identified as requiring action to improve ENISA's relevance, effectiveness, efficiency, coherence and added value in the future and ultimately help it contribute to increased NIS in the EU:

- *Weak institutional and legal framework for cybersecurity in the EU* – Cybersecurity is primarily seen as an area of national competence, while in reality it is an issue that transcends borders
- *Fragmentation of cybersecurity policy at EU level* – The fragmentation of cybersecurity policy is due to a number of EU-level actors in the area of cybersecurity and insufficient coordination

between them. One important factor here is the division of responsibilities between ENISA and CERT-EU.

- *Limitations for ENISA due to its size* – ENISA has difficulties to make an impact in the vast field of NIS as it has only limited human and financial resources to meet a broad mandate.
- *Limited visibility* – ENISA has not managed to develop a strong brand name and is not seen as a point of reference at European level for cybersecurity.
- *Not perceived as a proactive, visionary Agency* - ENISA's broad mandate makes it reactive to fulfilling the needs of as many stakeholders as possible, but this means that it loses focus. ENISA is not able to use its own knowledge to set work priorities due to the Member State dominance of the work programme.
- *A mandate that is not aligned with cybersecurity needs* – Cybersecurity threats have become a permanent issue in the EU and ENISA has been allocated long-term responsibilities (e.g. under the NIS Directive) which call for a permanent mandate.
- *ENISA does not sufficiently respond to the needs of all its stakeholders* – Under the current governance structure, the needs of the private sector are not sufficiently heard and thus are not adequately reflected in the Agency's work programmes.
- *ENISA should expand its activities to better respond to stakeholder needs* – There is a request by stakeholders (although not unanimous) to ensure a coherent ICT certification and standardisation system in the EU. Member States with fewer resources and expertise require additional support in receiving information on and assessing cybersecurity threats in order to respond to attacks.

Despite these issues, there is significant potential for ENISA, if sufficiently mandated and supported in terms of financial and human resources, to make a contribution to increased NIS in the EU. There is a clear need for cooperation and coordination across different stakeholders and ENISA as a decentralised EU agency is in the position to ensure a coordinated approach to cyber threats in the EU.

Options for the future of the Agency

Based on the key issues presented above – as derived from the findings and conclusions of the study - four options to review the current mandate of ENISA were developed. They are presented in Table 3 below, highlighting the specific factors for change that could be implemented under each of the options.

Table 3: Options for the future of ENISA

Option	Factor for change
Option 0: Baseline, maintain the status quo This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation[3] and Telecoms Framework Directive[4] would need to be taken into account.	**Revise ENISA's mandate to make its new tasks as per recent/upcoming legislation more specific:** • Involvement in Cooperation Group as required under the NIS Directive • CSIRT Network Secretariat • Electronic communication code, recital 92 (Telecoms Framework Directive) • eIDAS
Option 1: Expiry of ENISA's mandate (terminating ENISA) This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level.	N/A
Option 2: Enhanced ENISA (Keep ENISA with	**Strengthen ENISA's operational role:**

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[4] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

Option	Factor for change
changes to its mandate) This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.	• Provide periodic threat intelligence and ad hoc alerts • Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level • Provide emergency cybersecurity response
	Strengthen ENISA's role in policy development and implementation: • Render the consultation of ENISA by the Commission in cybersecurity matters obligatory • Formally involve ENISA in the Connecting Europe Facility • Establish regular meetings between ENISA and other agencies/international organisations
	Make ENISA's mandate permanent
	Strengthen ENISA's governance structure: • Increase the role of the Permanent Stakeholders' Group (PSG) • Allow ENISA more flexibility in the determination of its work priorities
	Include a role for ENISA in EU-level standardisation and certification: • Support the EU ICT Security Certification Framework • Support ICT security standardisation
	Strengthen ENISA's position relative to research and innovation: • Take part in programming implementation • OR Take part in programming in an advisory role • OR Benefit from EU research and development funding
	Increase ENISA's visibility: • Establish a liaison office in Brussels • Create a dedicated communications team within ENISA
Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity) This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.	**Create an EU cybersecurity umbrella:** • Such an umbrella would encompass ENISA and CERT-EU
	Create a virtual European CSIRT: • Coordinate CSIRT Network operations • Produce real time situational awareness and dynamic threat intelligence feeds • Maintain and provide own cybersecurity incident response capacity to public and private sector
	All factors related to Option 2 could be fulfilled under Option 3.

European Commission

Evaluation of ENISA
Luxembourg, Publications Office of the European Union

2017 – 10 pages

ISBN 978-92-79-72114-4
doi:10.2759/94930

KK-02-17-971-EN-N

doi:10.2759/94930

ISBN 978-92-79-72114-4

Error! Reference source not found.