EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 478 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the evaluation of the European Union Agency for Network and Information Security (ENISA)

1. INTRODUCTION

1.1 ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) was originally established in 2004 and had its mandate renewed periodically. The current ENISA mandate is set out in Regulation EU No. 526/2013[1] (the 'ENISA Regulation') and is due to expire on 19 June 2020.

ENISA's mandate is to contribute to a high level of network and information security within the Union. The ENISA Regulation outlines the specific objectives of the Agency, establishing that it shall:

- develop and maintain a high level of expertise.
- assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- use its expertise to stimulate broad cooperation between actors from the public and private sectors.

In addition, through the Directive EU No. 2016/1148[2] concerning measures for a high common level of security of network and information systems across the Union (the 'NIS Directive'), the EU co-legislators decided to attribute important roles to ENISA in the implementation of the law. In particular, the Agency provides the secretariat to the CSIRT Network (established to promote swift and effective operational cooperation between Member States), and it is also called on to assist the Cooperation Group for strategic cooperation in the execution of its tasks. In addition, the NIS Directive requires ENISA to assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practices.

The Agency is located in Greece, with its administrative seat in Heraklion (Crete) and the core operations in Athens. It has 84 staff members and an annual operating budget of €11.25m. It is headed by an Executive Director, with governance provided by a Management Board, Executive Board and Permanent Stakeholders Group. An informal Network of National Liaison Officers facilitates outreach with the Member States.

1.2 PURPOSE OF THE REPORT

Article 32 of the ENISA Regulation requires the Commission to undertake an evaluation of ENISA by 20 June 2018 *"to assess, in particular, the impact, effectiveness and*

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1495472820549&uri=CELEX:32013R0526
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

efficiency of the Agency and its working practices" and to consider whether the current mandate needs to be extended.

In light of the significant changes that occurred in the cybersecurity landscape since 2013, when the current ENISA Regulation was adopted – considering the achieved level of maturity at policy, market, technological level – in its 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[3], the Commission announced that it would advance the evaluation and review of ENISA. In particular, the Commission noted that the review of ENISA would provide an opportunity for a possible enhancement of the Agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience.

This vision was further confirmed in the 2016 Council Conclusions[4], which acknowledged that "cyber threats and vulnerabilities continue to evolve and intensify which will require continued and closer cooperation, especially in handling large-scale cross-border cybersecurity incidents". The conclusions reaffirmed that "the ENISA Regulation is one of the core elements of an EU cyber resilience framework" .

The results of the evaluation of ENISA fed into the impact assessment accompanying the proposal for a Regulation on the European Union Agency for Network and Information Security (ENISA, the "EU cybersecurity agency") and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

Pursuant art. 32 of the ENISA Regulation the Commission is to forward the evaluation report together with its conclusions to the European Parliament, the Council and the Management Board.This summary Report is accompanied by a Commission Staff Working Document on the evaluation of the European Union Agency for Network and Information Security (SWD(2017) 502).

2. MAIN FINDINGS OF THE EVALUATION

In compliance with the Better Regulation Guidelines of the Commission[5], the evaluation has assessed the effectiveness, efficiency, coherence, relevance and EU added value of the Agency, having regard to its performance, governance, internal organisational structure and working practices.

The analysis also took account of the evolved context where the Agency now operates, with regard in particular to: the new EU regulatory and policy framework (e.g. the NIS Directive, the Review of the EU Cybersecurity Strategy); the evolving needs of the Agency's stakeholders' community; and the complementarity and possible synergies with the work conducted by other EU and national institutions, agencies and bodies, such as the Computer Security Incident Response Team of the EU institutions, agencies and bodies (CERT-EU) and the European Cybercrime Centre (EC3) at Europol.

To evaluate the functioning of the Agency:

---

3 Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

4 Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

5 COM (2015)215final SWD (2015)111 final; http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf

- The Commission procured an independent study, which was carried out from November 2016 to July 2017, and which constitutes the main source of the evaluation together with internal analysis carried out by the Commission.
- The study activities included desk research, data collection and analysis including stakeholder surveys, in-depth interviews with key players in the cybersecurity fielda stakeholder workshop, benchmarking, positioning exercise of the Agency and a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis.
- The Commission also carried out a 12-week online public consultation, covering both the ex-post evaluation and the future of ENISA, as well as targeted consultations with key stakeholders.

The main findings of the evaluation, according to the evaluation criteria, can be summarised as it follows:

1. **Relevance:** In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU, ENISA's objectives proved to be relevant. In fact, 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. NIS continues to be a key political priority of the EU to which ENISA is expected to respond; however, ENISA's design as EU agency with a fixed-term mandate: (i) does not allow for long-term planning and sustainable support to Member States and EU Institutions in the rapidly changing cyber security threat landscape context; (ii) may lead to a legal vacuum as the provisions of the NIS Directive entrusting ENISA with tasks are of a permanent nature.

2. **Effectiveness:** ENISA overall met its objectives and implemented its tasks. It made a contribution to increased NIS in Europe through its main activities (capacity building, provision of expertise, community building, support to policy). It showed potential for improvement in relation to each. The evaluation concluded that ENISA has effectively created strong and trustful relationships with some of its stakeholders, notably with the Member States and the CSIRT community. Interventions in the area of capacity building were perceived as effective in particular for less resourced Member States. Stimulating broad cooperation has been one of the highlights, with stakeholders widely agreeing on the positive role ENISA plays in bringing people together. However, ENISA faced difficulties to make a big impact in the vast field of NIS. This was also due to the fact it had fairly limited human and financial resources to meet a very broad mandate. The evaluation also concluded that ENISA partially met the objective of providing expertise, linked to the problems in recruiting experts (see also below in the efficiency section).

3. **Efficiency:** Despite its small budget – among the lowest compared to other EU agencies – the Agency has been able to contribute to targeted objectives, showing overall efficiency in the use of its resources. The evaluation concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. One of the main challenges to the Agency's efficiency relates to ENISA's difficulties in recruiting and retaining highly qualified experts The findings show that this can be explained by a combination of factors, including the general difficulties across the public sector to compete with the private sector when trying to hire highly

specialised experts, the type of contracts (fixed term) that the Agency could mostly offer and the somewhat low level of attractiveness related to ENISA's location, for example linked to difficulties encountered by spouses to find work. A location split between Athens and Heraklion required additional efforts of coordination and were generating additional costs but the move to Athens in 2013 of the core operations department increased the agency's operational efficiency.

4. **Coherence:** ENISA's activities have been generally coherent with the policies and activities of its stakeholders, at national and EU level, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and other EU bodies has not been fully utilised. The evolution in the EU legal and policy landscape make the current mandate less coherent today.

5. **EU-added value:** ENISA's added value lied 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 provided by the Agency varied according to the diverging needs and resources of its stakeholders (e.g. big versus small Member States; Member States versus industry) and the need for the Agency to prioritize its activities according to the work programme. The evaluation concluded that a potential discontinuation of ENISA would be a lost opportunity for all Member States. It will not be possible to ensure the same degree of community building and cooperation across the Member States in the field of cybersecurity without a decentralised EU agency. The picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA.

3. CONCLUSIONS/RECOMMENDATIONS

The evaluation concluded that ENISA was entrusted by its Regulation with a broad mandate – which allows flexibility but in some instances lacks focus making it difficult for the Agency to achieve a big impact– and its objectives proved to be relevant during the period 2013-2016. The Agency managed to achieve good level of efficiency and showed the added value of acting at the EU level, in particular through key activities, such as the pan-Europan Cyber Exercises, the support to the CSIRTs community, the analyses on the threat landscape. ENISA contributed to increasing the network and information security in Europe mainly through supporting cooperation between Member States and NIS Stakeholders, as well as through its community and capacity building activities.

The Agency achieved these results despite several challenges presented in the previous sections of this report and the attached Staff Working Document. One of the key challenges was related to limited resources, which did not match the Agency's broad mandate, especially in view of the new tasks conferred to the Agency by the NIS Directive and the fast evolving threat landscape. ENISA also remains the only EU agency with a fixed-term mandate, despite, among others, tasks related to the NIS Directive as mentioned above.

The cybersecurity threat landscape is evolving fast with new threats emerging as Europe becomes ever more reliant on digital infrastructure and services through not only connected devices but now omnipresent connectivity. The Internet of Things creates new opportunities related to energy efficiency, environmental protection, connected mobility,

real time health monitoring and smart and seamless financial transactions in the digital economy and society. However in tandem with these business drivers are new vulnerabilities and exploits enabling compromised devices to disrupt the Digital Single Market.

The evaluation led to the conclusion that the current mandate does not equip ENISA with the necessary tools to face the current and future cybersecurity challenges.

In addition, there is now a growing risk of increased fragmentation at EU level due to a number of EU-level actors in the area of cybersecurity and insufficient coordination between them. The EU needs a focal point to address new threats which are horizontal in nature and impacting on multiple industrial sectors and to match the needs of the cybersecurity community, in particular the Member States, the EU institutions and the businesses. The evaluation suggests that there is a need for an EU Agency organised on a cross sectoral/horizontal basis with a strong mandate.

The evaluation shows that despite a number of challenging 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 cybersecurity in the EU.

There is also a clear need for cooperation and coordination across different stakeholders. The need for a coordinating entity at EU level to facilitate information flows, minimise gaps and avoid overlapping of roles and responsibilities becomes ever more acute. ENISA, as a decentralised EU agency and a neutral broker, is in the position to coordinate EU's approach to cyber threats.

On this basis, the Commission has put forward a proposal to reform ENISA, entrusting it with a permanent mandate that builds on the key strengths showed by the Agency and the new priority areas for action, for example in the area of cybersecurity certification. This new mandate should reflect the changed reality and empower the Agency to appropriately support the EU for the future.