ENISA Strategy

STATUS: APPROVED BY THE MB DECISION NO 2016/4

VERSION: 1.0

JANUARY 2016

Table of Contents

Prologue

In a constantly evolving digital environment, threats to the network and information systems in Europe are growing rapidly. While all economic and societal activities today rely upon information systems and communication networks, the development of European digital society can only be sustainably achieved with the establishment of proper network and information security (NIS) practices, policies, organizations and capacities.

As the European Union Agency for Network and Information Security, ENISA has actively contributed to the raising of awareness of NIS challenges in Europe since it was set up in 2004, to the development of Member States NIS capacities and to the reinforcement of the cooperation of Member States and other NIS stakeholders.

Whereas NIS has been set high in the EU political agenda notably in the European Cybersecurity Strategy (2013), the European Cyberdefence Policy Framework (2014) and in the European Digital Single Market (2015), ENISA will in the future, more than ever, need to accompany the efforts of Member States and Union institutions in reinforcing NIS across Europe. Above all, the recent adoption of the European directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security, further calls for enhanced commitment of ENISA in supporting a coherent approach towards NIS across Europe.

While ENISA should continue its well-established activities – from the support to the reinforcement of Member States national capacities to the organization of cyber crisis exercises – the adoption of the NIS Directive will require the development of further areas of action in order to accompany the evolution of NIS in Europe. ENISA will, in particular, play a key role in: steering the NIS operational cooperation by actively supporting Member States' CSIRTs' cooperation within the future European CSIRT network between the MS and the Institutions; providing input and expertise into policy level collaboration between national competent authorities in the framework of the Cooperation Group, supporting the reinforcement of the NIS of Union institutions in strong cooperation with CERT-EU and with the institutions themselves; ENISA will furthermore contribute to the reinforcement of NIS as a driver of the DSM and more generally of economic growth in Europe, including the development of NIS and related ICT industries in Europe.

While many Union institutions develop activities related to cybersecurity (Europol, European Defence, European External Action Service, Agency, etc.) ENISA aims to be the key point of reference for analysis and advice on NIS issues among Union institutions, entities and bodies and engage with relevant ones, in order to share its experience and expertise and support them in their activities. Furthermore, ENISA will support other stakeholders, in particular the private sector, to engage in Europe's efforts to ensure a significant improvement of the state of cybersecurity in Europe.

This paper provides ENISA's strategic vision which will ensure the coherence of its actions in years to come and significantly enhance its impact.

Introduction

Context

ENISA is the European Union Agency for Network and Information Security (NIS), established in 2004.

As set out in 2013 in its renewed mandate , ENISA has been set up "*for the purpose of contributing to a high level of Network and Information Security within the Union […] thus contributing to the establishment and proper functioning of the internal market*"[1], contributing to growth and employment in Europe.

The mission of ENISA is to contribute to *securing Europe's information society* by raising *"awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union*"[2].

In doing so, ENISA will act "*without prejudice to the competences of the Member States*" regarding their national security[3] and in compliance with the right of initiative of the European Commission.

In order to achieve its mission, several objectives and tasks[4] have been attributed to ENISA, *"without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security"*[5].

In line with these objectives and tasks, the Agency carries out its operations in accordance with an annual and multiannual work programme, containing all of its planned activities, drawn up by the Executive Director of ENISA and adopted by ENISA's management board (MB).

ENISA's approach is strongly impact driven, based on the involvement of all relevant stakeholder communities. The Agency also provides the Union institutions, bodies and agencies (hereinafter: "Union institutions") and the Member States with a mechanism allowing them to call upon its services to support their NIS capability development[6], resulting in a more agile and flexible approach to achieving its mission.

Purpose

In the light of its recommendations on NIS strategies[7] and with a view to offering a focused and coherent implementation to its mandate, this document defines a strategy for ENISA (hereinafter "the strategy") identifying long term core priority objectives for the Agency and presenting them in a structured and concise manner.

In a more practical way, the strategy will

- Support ENISA's Executive Director and MB in the elaboration and adoption of consistent multiannual and annual work programmes[8]. As a consequence, the four objectives detailed below, will provide long

[1] Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013, article 1(1).
[2] Article 1(1) of ENISA Regulation (EU) No 526/2013
[3] Article 1(2) of ENISA Regulation (EU) No 526/2013
[4] Article 2 and 3 of ENISA Regulation (EU) No 526/2013
[5] Article 1(2) of ENISA Regulation (EU) No 526/2013
[6] Article 14 of ENISA Regulation (EU) No 526/2013
[7] "An evaluation framework for cybersecurity strategies" (2014), "National cybersecurity strategies: an implementation guide" (2012), "National cybersecurity strategies: current status of cybersecurity strategies within the European Union"
[8] Annual and multiannual work programmes referred to in the Article 5 §2 of ENISA Regulation (EU) No 526/2013

term strategic objectives to ENISA, to help in prioritizing and focus activities on a multi-annual and annual basis and will offer a stable structure for these documents[9].

- Guide ENISA's management and staff in the implementation of their activities.

The strategy is established for an indicative period of 5 years until the end of the current mandate (June 2020)[10]. Should the mandate undergo an anticipated revision, or otherwise beyond this 5 years period, the strategy will be updated, following a careful evaluation of its implementation.

The strategy should be made public on ENISA's website, after formal adoption by the MB.

Summary of the strategic objectives

ENISA's strategic objectives are derived from the ENISA regulation, inputs from the Member States and relevant communities, including private sector.

In cooperation and in support to the Member States and the Union institutions, ENISA will in priority seek to achieve:

#Expertise - **Anticipate and support Europe in facing emerging network and information security challenges**, by collating, analysing and making available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

#Policy - **Promote network and information security as an EU policy priority**, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.

#Capacity - **Support Europe maintaining state-of-the-art network and information security capacities**, by assisting the Member States and European Union bodies in reinforcing their NIS capacities.

#Community - **Foster the emerging European network and information security community**, by reinforcing cooperation at EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector.

#Enabling - **Reinforce ENISA's impact**, by improving the management of its resources and engaging more efficiently with its stakeholders, including Member States and Union Institutions, as well as at international level.

[9] In order to achieve the 5 year strategic objectives laid out in this document, the multiannual work programme will provide prioritized mid-term operational objectives to be achieved by ENISA within a period of 3 years. Annual concrete activities (*outputs*) will be identified in the annual work programmes, according to a recursive approach in order to achieve the mid-term operational objectives and in the long term the strategic objectives.
[10] Article 36 of ENISA Regulation (EU) No 526/2013

1. #Expertise – Anticipate and support Europe in facing emerging network and information security challenges

Activity: In order to achieve this objective, ENISA will collate, analyse and make available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

ENISA will collate, analyze and make available information on global cyber issues with a view to developing insights on issues of high added-value for the EU. In this analysis, ENISA will cover both existing as well as new technologies and their integration, such as smart infrastructures, Internet of Things, Cloud and Big Data and evaluate their impact on NIS and related challenges such as NIS aspects of data protection.

To that end, ENISA will bring together Member States relevant stakeholders, such as industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security, and representatives of national regulatory authorities[11] related to NIS in order to discuss and explore NIS problems and challenges that they have encountered.

By compiling, comparing and evaluating these experiences alongside publicly available data, ENISA will help to anticipate future risks and threats and identify those technologies and services that pose specific security challenges in particular with regard to critical infrastructures, businesses at large and citizen's private data.

In response to this the agency will develop and disseminate best practices which can be used to inform across a number of different horizontal fields including research and development, innovation, standardization, IT Security certification and other relevant industrial practices.

[11] Article 12(2) of of ENISA Regulation (EU) No 526/2013

2. #Policy – Promote network and information security as an EU policy priority

Activity: In order to achieve this objective, ENISA will assist and advise the Union institutions and the Member States in developing and implementing EU policies, guidance and law on all matters relating to NIS.

Building upon its expertise gathered while achieving objective 1, ENISA will assist and advise the Union institutions and the Member States in:

- **Developing European NIS related policies and laws.** To this end, ENISA will proactively engage with Union institutions, and in particular all relevant DGs of the European Commission, in order to advise, including by providing preparatory work, advice and analyses relating to the development and update of Union NIS policy and law.
  In cooperation with the Member States, in particular as part of the work of the Cooperation group, as well as with other relevant public and private stakeholders, ENISA will promote a vision on how to significantly strengthen NIS across the EU, using adequate EU policy levers. ENISA will, in particular, promote the inclusion of NIS aspects within policies including – directly or indirectly – a digital dimension. ENISA will also actively contribute to the reinforcement of NIS as a driver of the DSM and more generally of economic growth in Europe, including the development of NIS and related ICT industries in Europe.
- **Implementing, at EU level, NIS related policies and law, following their adoption.** While ENISA, focusing in particular on the implementation of the NIS Directive[12], will support cooperation among Member States regarding EU policies and law including a NIS dimension in order to foster consistent EU-wide approach to their implementation. ENISA will bring together Member States and other relevant public and private stakeholders, and will seek to produce recommendations taking into account their needs and constraints (national, sectorial).[13]

[12] Proposal for a Directive of the European parliament of and of the Council concerning measures to ensure a high common level of network and information security across the Union

[13] This objective should not be confused with ENISA's support provided to single Member States requesting assistance pursuant to Art. 14 of ENISA Regulation (EU) No 526/2013 in implementing EU regulations' specific provisions at national level, as part of objective 3 regarding ENISA's support to capacity building.

3. #Capacity – Support Europe in maintaining state-of-the-art network and information security capacities

Activity: In order to achieve this objective, ENISA will assist the Member States and Union institutions in reinforcing their NIS capacities.

ENISA will support capacity building across the Union to make national public and private sectors and the Union institutions' networks more resilient and secure. This will involve working closely with Member States and liaising, in cooperation with them, with various different stakeholders across the Union to develop skills and competencies in the field of NIS. ENISA will focus its effort on the following actors:

- **Member States:** ENISA will support the development of Member States' national NIS capabilities by providing recommendations on key dimensions of NIS capacity building and will focus in priority on those highlighted in the NIS Directive, including on the development and efficient functioning of National/Governmental CSIRTs and policy level collaboration between national competent authorities in the framework of the Cooperation Group, the development of national strategies, the establishment of necessary national frameworks to aid implementation of national incident reporting schemes and on training to improve skills. ENISA will as well offer, upon their request, direct to support to single Member States[14]. To that end, the Agency will develop proactive relationships with Governments across the EU.
- **Private sector:** ENISA will support Member States to engage with private sector on their NIS, encouraging companies to take a whole-business approach to cyber threats from the top of the board down. ENISA will also work with private sector stakeholders to help improve cyber security of networks within companies.
- **Union institutions:** in close coordination with the Union institutions, ENISA will support them in reinforcing and coordinating their NIS capabilities and to that end, will establish a close and sustainable partnership with CERT-EU. As part of this mission, ENISA will advise on key orientations and, upon request, on actions to be implemented in order to achieve a high level of NIS across all Union institutions. ENISA will, also, produce with CERT-EU information notes on threats and risks with a view to making the EUIs and agencies more secure. ENISA will, whenever this is adequate, build on experience gained by CERT-EU and the Union institutions to contribute to the broader EU NIS community.
- **Citizens:** alongside Member States, ENISA will help EU citizens to gain essential cyber security knowledge and skills to help protect their digital lives. This will include promoting an annual European Cyber Security month and working with the Member States delivering projects like the Cyber Security Challenge as well as national initiatives, upon request from a Member State.

While aiming at supporting different types of actors, ENISA will take into account the transversal aspects of NIS capacity building such as activities supporting the increase of the number of NIS experts in Europe (e.g. academic training) and the spread of basic cyber hygiene in public and private organizations as well as in the general public.

[14] Article 14 of ENISA Regulation (EU) No 526/2013

4. #Community – Foster the emerging European network and information security community

Activity: In order to achieve this objective, ENISA will enhance cooperation at EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector.

Beyond its support to the development and the implementation of EU NIS related policies (objective 2) and to Member States and Union institutions towards the development of their NIS capabilities (objective 3), ENISA will actively support cooperation at EU level on NIS.

ENISA will in particular seek to support in priority:

- **CSIRT cooperation among the Member States**, by supporting voluntary cooperation among Member States CSIRTs, within the CSIRT network established by the NIS Directive. As part of this activity, ENISA will provide the secretariat of this network and actively support its functioning by suggesting ways to improve cooperation among CSIRTs and supporting this cooperation, including by developing and providing guidance on best practices in the area of operational community efforts, such as on information exchange.
- **Cyber crisis cooperation among Member States**, by continuing to support the organization of the Cyber Europe exercises which shall remain one of ENISA's key priority activities, while ensuring adequate synergies with the CSIRT network.
- **Dialogue among NIS related communities**, including between CSIRTs and law enforcement and data privacy communities, in order to support consistent EU-wide approach to NIS. To that end, ENISA will continue to interact with Europol (EC3).
- **Dialogue among public and private sectors on relevant NIS issues of European general interest,** in particular with a view to contribute to the objectives of the Digital Single Market, such as stimulating the development and the competitiveness of NIS and ICT related industries and services in Europe.

5. #Enabling – Reinforce ENISA's impact

Activity: In order to achieve this horizontal objective, ENISA will improve the management of its resources and engage more efficiently with its stakeholders, including Member States and Union institutions, as well at international level.

5.1 Management

The Agency will act according to the following key general principles and rules:

- **ENISA will ensure a responsible financial management of its resources.** In the next five years, ENISA will continue to improve processes for monitoring financial flows and expects to maintain high commitment and payment rates.
- **ENISA will guarantee a high level of transparency regarding its internal processes** and way of working.
- **ENISA will increase and maintain internal IT-security expertise** within the Operational Department, with a view to lowering the need to rely upon external expertise while improving its ability to steer the work of external experts, in particular in developing and maintaining a high level of expertise (objective 1 of the ENISA Regulation)[15].

5.2 Engagement with stakeholders

- **ENISA will continue to improve the quality and effectiveness of its relations with Member States' NIS competent authorities.** ENISA will, in particular, make it easier for the national competent authorities to engage with the Agency, while offering better visibility on its activities. To this end, ENISA will define Standard Procedures regarding the principles and modalities of the participation and consultation of national competent authorities and other NIS related communities as part of its activities. It will also engage with the national competent authorities actively participating in the work of Cooperation Group established by the NIS directive. ENISA will also establish an updated list of its ongoing and future activities, including relevant contact and calendar information for Member States and NIS communities to facilitate their engagement with ENISA.
- **ENISA will reinforce and structure its cooperation with all Union institutions, entities and bodies** on NIS related issues, in particular the European Commission, as well as CERT-EU on the NIS of the Union institutions, and Europol (EC3) with regard to community building between national NIS and law enforcement communities.
- **ENISA will continue to improve the quality and effectiveness of its relations with other relevant stakeholders**, such as NIS and ICT related industries and services, essential operators, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security.
- **While developing its expertise, ENISA will avoid duplicating existing work at National level** and will focus on issues of real-added value for Europe.

[15] Article 2 of ENISA Regulation (EU) No 526/2013

5.3 International activities

- **ENISA will act at international level according to EU and Member States' external policies and guiding principles to be defined and adopted by the MB.** ENISA's international relations should primarily aim at supporting EU's external policy initiatives including a cyber dimension and promoting the EU and its NIS expertise outside its borders.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu