ENISA’s Position on the NIS Directive

1 Introduction

This note briefly summarises ENISA’s position on the NIS Directive. It provides the background to the Directive, explains its significance, provides an overview of the content and discusses the implications for ENISA.

2 Background and next steps

The current approach to CIIP and resilience within the EU has its roots in the Commission communication of 2009, entitled ‘Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience ‘[1], together with a number of associated policy documents that essentially build upon and refine this approach.[2][3][4]

In 2013, the Commission released the Cybersecurity Strategy of the EU[5], which laid out a number of fundamental principles underlying the EU approach to cybersecurity, followed by 5 strategic priorities. The proposal for the NIS Directive is made under the first strategic priority ‘Achieving Cyber resilience’.

Between 2013 and 2015, the Directive was discussed intensively by the Commission, the Parliament and the Council. The European institutions reached an informal political agreement on the NIS Directive on December 7, 2015. Member States (the Committee of Permanent Representatives (COREPER)) endorsed this agreement on December 18. On January 14, the European Parliament’s IMCO committee voted in favour of the NIS Directive (34-2).

The Directive will now be voted at an EU Parliament plenary session in the coming months (mostly expected in April). After the date of entry into force Member States will have 21 months at their disposal to transpose the laws, regulations and administrative provisions necessary to comply with the Directive.

3 Significance

Once adopted, the NIS Directive will be the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. This in itself represents a very significant step in the approach to securing EU information systems.

[1] Commission Communication of March 2009, “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, COM(2009)149.

[2] "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

[3] Council resolution of 18 December, 2009 ‘On a collaborative approach to network and information security (2009/C 321 01)

[4] Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

[5] Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

By imposing a certain number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity *'with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market'*

4 Overview of Content

The main points of the NIS Directive can be summarised as follows:

- **Governance**: Member States must develop an NIS Strategy and designate the appropriate competent authority/ies to deal with the NIS maters at national level
- **Mandatory information sharing/exchange**: Member States are required to exchange information on good practices and incidents via the CSIRT[6] network and the co-operation network (both defined in the NIS Directive)
- **Reporting of incidents of significant impact**: operators of essential services (e.g. health, energy, transport, etc.) are required to report incidents of significant impact at their national NIS competent authority.

More specifically Member States are required to:

- Produce and maintain a National NIS Strategy.
- Designate one or more national competent authorities on the security of network and information systems.
- Designate one or more Computer Security Incident Response Teams (CSIRTS)
- Assign representatives to contribute to the 'cooperation network' that will be established to support and facilitate strategic cooperation among Member States.
- Ensure that representatives of the Member States' CSIRTs participate in the 'CSIRTs network'
- Ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations.
- Ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations.
- Ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in the context of offering services.
- Ensure that the competent authorities take action, if necessary, through ex post supervisory activities, when provided with evidence that a digital service provider does not meet the requirements laid down by the Directive.
- Encourage the use of European or internationally accepted standards and/or specifications relevant to security of networks and information systems.
- Lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented.

[6] CSIRTs in the context of the NIS Directive means CERTs.

5 Implications for ENISA

The implications for ENISA of the NIS Directive are summarised below.

5.1 Co-operation Group

ENISA will be a member of the strategic Co-operation Group. The Commission will act as secretariat to this group, which will consist of representatives of the Member States, the Commission and ENISA.

The objective of the group is to support and facilitate strategic cooperation among Member States in order to achieve an equal level playing field for all Member States.

ENISA will assist the cooperation group in its tasks when requested to do so by the members. The Agency will also proactively guide the group by sharing the knowledge and experience gained through the execution of its work programmes, but the right of initiative is with the group itself.

Areas in which ENISA is particularly qualified to offer assistance are as follows:

- Providing strategic input for the definition of minimum security requirements for public and private sector
- Helping Member States to meet these requirements
- promoting sharing of good of practices among Member States on specific topics
- Executing targeted studies on specific topics on behalf of the cooperation group.

5.2 CSIRT Network

Through Article 8b, the NIS directive establishes a CSIRTs network "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". This group is composed of representatives of the Member States’ CSIRTs and CERT-EU and ENISA will act as the secretariat.

The CSIRTs Network provides a forum where Member States' National CSIRTs can cooperate, exchange information, and also build trust. Member States CSIRTs will be able to improve the handling of cross-border incidents, and even discuss how to respond in a coordinated manner to specific incidents. The CSIRTs Network could also provide a mechanism to enable Member States to participate more actively in cyber exercises like ENISA's CyberEurope.

ENISA is also asked to proactively support the cooperation among the CSIRTs. Hence, in contrast to its role in the cooperation group, ENISA is expected to take the initiative to guide the CSIRT group in the fulfilment of its duties. The Agency will organise meetings of the CSIRTs Network, and provoke discussion by proposing discussion topics. It will also provide its expertise and advice both to the Commission and Member States, either in the form of guidance or in answer to specific requests.

In supporting the CSIRTs network, ENISA will leverage previous work (such as the ongoing cooperation with Europol’s EC3 Agency, where ENISA facilitates the coordination between relevant authorities and law enforcement agencies). At the request of a Member State, the Agency can also support the Member States in developing a National CSIRT.

In the recitals of the Directive, the secretariat of the CSIRT network is encouraged to maintain a website or host a dedicated page on an existing website where general information on major NIS incidents occurring across the EU is put at the disposal of the general public, with a specific focus on the interests and needs of businesses.

5.3 Incident Reporting for Digital Service Providers & Essential Service Providers

ENISA will support Member States in developing the incident reporting framework for both essential and digital service providers (DSPs). Given the differences in the sectors mentioned in the Directive we would recommend to develop a generic reporting framework and a sector specific component that would customise the generic scheme, thus achieving consistency across sectors.

ENISA has significant expertise on incident reporting at the EU level through the work carried out with Member States and telecoms providers on the transposition of Article 13a of the Telecommunications framework Directive of 2009. The Agency also contributed to the interpretation of Article 19 of the eIDAS regulation and now helps trust service providers in implementing this article.

ENISA encourages the cooperation group to build on this experience and knowledge when deciding on the implementation strategy for Articles 14 and 15a of the Directive (security requirements and incident notification for operators of essential services and digital service providers respectively). More specifically ENISA can assist Member States to agree on the parameters and thresholds upon which an incident is considered significant, the reporting framework and the information to report as well as the ex-post analysis of the reported data. In this context, ENISA could help Member States to align different reporting schemes across sectors and across geographical borders, thereby making sure they remain simple, pragmatic and relevant for both public and private sector without increasing the cost of operation.

5.4 Identification of Essential Operators

ENISA expects to assist the Member States in identifying operators of essential services. ENISA can take stock of the different approaches already in use by a few Member States and then develop a common approach that could be used by all.

5.5 Minimum Security Requirements for Digital Service Providers & Essential Service Providers

Building on its CIIP program and the knowledge and expertise acquired around this on several essential sectors ENISA is uniquely positioned to assist Member States and the private sector in defining minimum security requirements for digital service providers and essential service providers.

Should the Agency be asked to do so, ENISA will engage relevant public and private stakeholders for each essential sector, inventory existing good and common practices and standards, analyse their appropriateness and compare with other state of the art methods and then propose a set of requirements. The proposed requirements would need to be extensively validated to make sure the end result raises the level of cyber security in the sector without increasing the cost of operation for essential operators.

In that context ENISA can also help Member States in devising criteria for declaring operators as essential.

5.6 National Cyber Security Strategies

The NIS Directive requests Member States to establish and execute a national NIS Strategy. The description of what constitutes such a strategy is largely compatible with the term National Cyber Security Strategy (NCSS) as used by ENISA.

ENISA has worked together with the Member States to develop good practices on how to achieve this and coordinates an active network of Member States that share expertise and knowledge on good practices in this area. For this reason, the Agency expects to continue supporting Member States in their efforts to define, implement and maintain the national NIS Strategies referred to by the NIS Directive.

However, given the state of maturity of this particular area, it is not seen as a priority in the short term.

5.7 Standardization and certification

The NIS Directive highlights the importance of establishing a body of common standards and conformity assessment frameworks in order to achieve a consistent level of information security in Europe. Standards and their conformity assessment are referred throughout the Directive, as well as the role of ENISA in facilitating the application of the provisions related to these areas.

Recital (32) of the NIS Directive argues that:

- In order to ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level.
- ENISA should assist Member States through advice and guidelines.
- To this end it might be helpful to draft harmonised standards, which should be done in accordance with relevant European legislations.

Article 15a of the NIS Directive, on security requirements and incident notification, establishes that compliance with international standards shall be taken into account in order to ensure a level of security of network and information systems appropriate to the risk presented.

Article 16 of the NIS Directive, on standardization, encourages the use of European or internationally accepted standards and/or specifications relevant to security of networks and information systems, and determines that ENISA shall, in cooperation with Member States, elaborate advice and guidelines regarding the technical areas which should be considered for standard adoption.

ENISA has been involved for some years now in discussions among stakeholders towards defining a common strategy to ICT security standardization and certification in Europe. The Agency has conducted a series of activities on these areas, such as consultation workshops and policy studies, involving participants both from the public and private sectors. As such, ENISA is well positioned to launch and support discussions towards all aspects related to standardization and certification in the NIS Directive. The envisioned role involves initiating discussions towards a common framework for the certification of ICT security products in Europe, followed by undertaking the necessary activities to coordinate and support the implementation of such a common framework. Once a framework is established, ENISA should have a supporting role to ensure coordination and dialog among all EU stakeholders.

6 Conclusions

As a result of the work it has carried out in the past, ENISA is ideally positioned to assist the Member States in implementing the NIS Directive once it is adopted. This note has provided a number of arguments explaining how this can be achieved in practice for specific requirements raised by the Directive.