NIS Directive and national CSIRTs

1 Introduction

In December 2015, the Commission, the Parliament of the EU, and the Council of Ministers reached an agreement on the Network and Information Security (NIS) Directive (hereafter "the Directive"). This draft Directive still needs to be polished, but a preliminary version is already available. Articles and paragraphs referred to in this document refer to the draft version of the Directive mentioned here. The final text is expected in spring. This document will be adjusted should the NIS Directive change.

This note explains the structure of the Directive, and highlights the parts that are relevant to National CSIRTs. For easier reading we refer to national CSIRTs in the context of this document simply as "CSIRT" or "dedicated CSIRT".

2 Structure of the Directive

The Directive is structured around the following sections. More specific provisions directly targeted to CSIRTs (mainly from Chapter 3 and Annex 1) will follow in Section 3:

Recitals give the context in which the Directive works. They state the importance and specificities of Network and Information Security, and describe the actors that will need to play a role.

Chapter 1. General provisions. This Chapter describes the goals of the Directive, and its legislative environment. It also gives formal definitions to terms that appear in the text.

Chapter 2. National frameworks on NIS. This Chapter lists the different entities and legislative frameworks that each Member State will have to set up in order to comply with the Directive. Each MS needs to adopt a national NIS strategy; designate one or more national competent authorities, as well as a single point of contact for cross-border cooperation; and set up at least one Computer Security Incident Response Team (CSIRT). These teams need to cover certain sectors and services.

***Chapter 3**. Cooperation between competent authorities. This Chapter defines two groups meant to improve NIS-related cooperation between MS. The first is the Cooperation Network, composed of representatives of MS, the Commission, and ENISA. This group is meant to focus on strategic issues. The second group is the CSIRT Network, composed of representatives of MS' CSIRT and CERT-EU, with the Commission as observer and ENISA as Secretary and active support.*

Chapter 4. Security of the NIS of operators of essential services. This Chapter defines security requirements for and duties of operators of essential services. These services are described in Annex 2 of the Directive.

Chapter 4a. Security of the NIS of digital service providers. This Chapter defines security requirements for and duties of digital service providers. These providers are described in Annex 3 of the Directive.

Chapter 4b. Standardisation. This Chapter encourages the use of EU standards.

Chapter 5. Final provisions. This Chapter covers all other aspects, like the details the timeline for transposition of the Directive, or penalties.

***Annex 1**. Requirements and tasks of the CSIRT. This Annex gives a list of tasks that a MS' CSIRT has to perform.*

Annex 2. Sectors and entities. This Annex lists the sectors and subsectors that need to be covered by each country's Information Security Strategy and CSIRTs.

Annex 3. Types of digital services. This Annex lists the digital services targeted by the Directive.

3 CSIRTs

Article 7 of the Directive gives the framework for CSIRTs. The following table presents each paragraph, and if necessary comments on what it means for the relevant CSIRTs.

PARAGRAPH	STATEMENT	MEANING
1	Each Member State shall designate one or more Computer Security Incident Response Teams (hereinafter: "CSIRTs ") covering at least the sectors referred to in Annex II and types of digital services referred to in Annex III, responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CSIRT may be established within a competent authority.	Each MS will designate one or more CSIRT. Together, these CSIRTs need to cover the sectors and services listed in Annex II and III. The designated CSIRT(s) need to fulfil the requirements and tasks listed in Annex I. This is one of the places where the Directive points to "adequate resources and equipment" for the CSIRT.
1a	Where they are separate, the competent authority, the single point of contact and the CSIRTs of the same Member State shall cooperate with regard to the obligations laid down in this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services pursuant to Article 14(2) and (2ac) or by digital service providers pursuant to Article 15a(2).	The Directive does not impose a structure or hierarchy for the competent authority, the single point of contact and the CSIRTs. They may be together in one organisation, or be separate. What matters is that, together, they have to fulfil the obligations defined by the Directive. Each Member State will have to come up with the structure that suits them. The designated CSIRTs are entitled to data on incidents notified by operators of essential services and providers of digital services.
2	Member States shall ensure that the designated CSIRTs have adequate resources to effectively carry out their tasks set out in point (2) of Annex I.	The designated CSIRTs are entitled to sufficient resources, which need to be provided by the respective government of the Member State. This is the second time the Directive points to "adequate resources and equipment" for the CSIRT
3	Member States shall ensure that the designated CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.	The third time the Directive points to "adequate resources and equipment" for the CSIRT
4	Member States shall inform the Commission about the remit as well as the main elements of the incident handling process of the CSIRTs.	CSIRTs need to document their constituencies and services. They also will need to provide a high level overview of their incident handling process to the Commission. The practical details as to how this will happen are not defined yet, however a good start is that the team publishes an RFC2350-compliant document (https://tools.ietf.org/html/rfc2350).
5c	Member States may request the assistance of ENISA in developing national CSIRTs.	CSIRTs can get ENISA's help either to set up their operations, integrate in the community, or ask for

PARAGRAPH	STATEMENT	MEANING
		training. Please contact cert-relations@enisa.europa.eu for more details.

4 The CSIRT Network

Article 8b of the Directive covers the CSIRT Network.

PARAGRAPH	STATEMENT	MEANING
1	In order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.	There will be a dedicated network for all national CSIRTs established, run by the MS (with the help of ENISA) and secretariat provided by ENISA.
2	The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. The European Network and Information Security Agency (ENISA) shall provide the secretariat and actively support the cooperation among the CSIRTs.	ENISA is there to support the group and its members. The Agency will provide resources and input to discussions.
3	The CSIRTs network shall have the following tasks:	Exactly how the group will perform these tasks is up to the group itself, as stated by paragraph 5. It means that the group will determine its own priorities, with input from the Collaboration Group. ENISA will support the group by making appropriate proposals.
3a	Exchange information on CSIRTs services, operations and cooperation capabilities	(see comment for paragraph 3)
3b	At the request of the representative of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident and associated risks. Any Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident.	(see comment for paragraph 3)
3c	Exchange and make available on a voluntary basis non-confidential information on individual incidents.	(see comment for paragraph 3)
3d	At the request of the representative of a Member State's CSIRT, discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.	(see comment for paragraph 3)
3e	Support Member States in addressing cross-border incidents on the basis of their voluntary mutual assistance.	(see comment for paragraph 3)
3f	Discuss, explore and identify further forms of operational cooperation, including in relation to: (i) categories of risks and incidents (ii) early warnings	(see comment for paragraph 3)

PARAGRAPH	STATEMENT	MEANING
	(iii) mutual assistance (iv) principles and modalities for coordination, when Member States respond to cross border NIS risks and incidents.	
3g	Inform the Cooperation Group on its activities and on the further forms of operational cooperation discussed pursuant to paragraph 3(f), and request guidance related thereto.	(see comment for paragraph 3)
3h	Discuss lessons learnt from NIS exercises, including from those organised by ENISA.	(see comment for paragraph 3)
3i	At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT.	(see comment for paragraph 3)
3j	Issue guidelines in order to facilitate the convergence of (operational) practices with regard to the application of the provisions of this Article concerning operational cooperation.	(see comment for paragraph 3)
4	As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall every one and a half years produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this article. That report shall also be submitted to the cooperation group.	The form and content of the report are not defined yet. This will need to be negotiated between the CSIRT network and the cooperation group. ENISA will help producing the report, and the group will have to approve it.
5	The CSIRTs network shall define its own rules of procedure.	The group will need to determine its governance structure and terms of reference. ENISA, as secretary and support, can provide input to the group and come up with proposals

5 Tasks for CSIRTs (Annex 1)

Annex 1 of the Directive gives basic requirements for designated CSIRTs, as well as a list tasks.

PARAGRAPH	STATEMENT	MEANING
Preamble	The requirements and tasks of the CSIRT shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements	This is a tool for designated CSIRTs to demand that their mandate be officially published. ENISA and others have long argued that an officially recognised mandate is one of the very first steps for a successful national CSIRT.
1	Requirements for the CSIRT	Article 1 is about operational requirements, and gives arguments to request necessary budget, manpower, or infrastructure.
1a	The CSIRTs shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others at all times. Furthermore, the	There are two parts to this requirement: 1. High availability of communication services. Without further details, it's hard to provide

PARAGRAPH	STATEMENT	MEANING
	communication channels shall be clearly specified and well known to the constituency and cooperative partners	much guidance. *In fine*, it will be up to the CSIRT Network to define what constitutes high availability. ENISA will support the group by making appropriate proposals. 2. Clear specification of communication channels. RFC 2350 is the industry standard for publishing contact information. ENISA recommends that all participating CSIRTs publish such a document.
1c	The offices of the CSIRT and the supporting information systems shall be located in secure sites.	The group will have to define what "secure site" means: depending on the context, the range of measures that can be taken is huge. ENISA will support the group by making appropriate proposals.
1e	Business continuity: 1. The CSIRT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers, 2. The CSIRT shall be adequately staffed to ensure availability at all times, 3. The CSIRT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be available.	1. This requirement can be translated as the need for adequate tools to track incidents. There is a variety of tools that CSIRTs can use. Popular tools are RTIR, FIR, etc. More concrete definitions are up to discussion within the CSIRT network. ENISA will support these discussions by making appropriate proposals. 2. See ENISA CSIRT maturity study as a first pointer, but more concrete definitions are up to discussion within the CSIRT network. ENISA will support these discussions by making appropriate proposals. 3. See 1a
1f	CSIRTS shall have the possibility to participate, where appropriate, in international cooperation networks	We interpret this as a tool for designated CSIRTs to make sure they have the necessary travel budget to take part in existing communities like TF-CSIRT, FIRST, or EGC. In order to contribute to that and make it easier for designated CSIRTs, ENISA will try as much as possible to co-locate physical meetings of the group with TF-CSIRT meetings.
2	Tasks of the CSIRT	Article 2 is about what designated CSIRTs will have to do. This should be considered as the minimum set of tasks for designated CSIRTs.
2a	Tasks of the CSIRT shall include at least the following: 1. Monitoring incidents at a national level, 2. Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents, 3. Responding to incidents, 4. Providing dynamic risk and incident analysis and situational awareness, 5. Participating in the CSIRT network	1. Monitoring is a generic term, and designated CSIRTs will need to translate it to their own context. ENISA plans to make monitoring the topic of its Workshop for national and governmental CSIRTs in May 2016. 2. This task amounts to providing the "Alerts and Warnings" and "Announcements" services. More information as to how a CSIRT can deliver these services can be found in ENISA's guides on (Set up; Alerts-Warnings-Announcements?) 3. This is a basic requirement for CSIRTs. If necessary, ENISA's Incident Management Guide can be of help.

PARAGRAPH	STATEMENT	MEANING
		4. Concrete definitions are up to discussion within the CSIRT network. ENISA will support these discussions by making appropriate proposals. 5. Participation, both online and in physical meetings, is essential to build trust between the members of the group.
2b	The CSIRT shall establish cooperative relationships with private sector.	Collaboration with the private sector is required to handle incidents efficiently. Designated CSIRTs will need to cover at least the sectors specified in Annex II of the Directive, however the group members will have to decide what information they want to share with the private sector. ENISA will support the group by making appropriate proposals.
2c	To facilitate cooperation, the CSIRT shall promote the adoption and use of common or standardised practises for: 1. incident and risk handling procedures, 2. incident, risk and information classification schemes.	More concrete definitions are up to discussion within the CSIRT network. ENISA will support these discussions by making appropriate proposals.

6 Conclusion

The advent of the NIS Directive is a significant event in the EU, because it is the first time NIS is tackled at such a high level.

For designated CSIRTs, the Directive gives many arguments that will help them formalise their mandate as well as secure budget, resources, and infrastructure.

The tasks given to the CSIRT network are varied, and it will be up to group members to define their own rules and good practices. The group can help build further trust within CSIRTs in the EU, provided its members take an active part.

ENISA will provide active support to the group, as Secretary, but also in helping teams come to meetings, and by providing input for discussions and moderating debates if necessary.

About “Info Notes” from ENISA

With the “Info Notes” series ENISA aims at giving the interested reader some background and recommendations about NIS related topics. The background and recommendations are derived from past experiences and common sense, and should be taken as starting points for discussions on possible course of action by relevant stakeholders. Feel free to get in touch with ENISA to discuss or inquire more information on the “Info Notes” series (cert-relations@enisa.europa.eu).