Gaps in NIS standardisation

Recommendations for improving NIS in EU standardisation policy

V. 1.0

NOVEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank all those who contributed to this study and reviewed it, specifically the members of various Standard Developing Organisations.

ISBN: 978-92-9204-186-1
doi: 10.2824/975760 Catalogue number: TP-06-16-337-EN-N

Table of Contents

Executive Summary

This report recommends that the European Commission, with the support of the Member States, pursuant to the NIS Directive, adopt a standards based framework for the exchange of threat and defensive measure information that impacts the functioning of Network Information Infrastructure (NII). The capabilities from this framework underscore NII as Critical Infrastructure of the EU and its Member States.

This report recognizes the work already addressed by a number of European bodies including the designated European Standardization Organisations (CEN, CENELEC and ETSI) and the Cyber Security Focus Group (CSCG), the European Reference Network for Critical Infrastructure Protection (ERNCIP), and individual Member States who have already taken steps to facilitate information sharing between Computer Security Incident Response Teams (CSIRTs). The recommendations of this report include extending the technical basis for information sharing in the following ways:

- Adopting open standards in threat exchange based on the globally accepted STIX/TAXII/CyBOX platform to be prepared as an European Norm (EN) defining the syntax and semantics of the data and the necessary transfer protocol, and an accompanying guide to the implementation of the standard
- Extending the risk analysis and defensive measures capabilities defined in current standards to allow Member States to address the NII and NIS provisions necessary to mitigate risk both at national and regional level. This should be prepared as an EN extending the capabilities already described in ETSI TS 102 165-1, ETSI TR 103 305, ISO/IEC 15408 and in relevant ISO/IEC JTC1 2700x series standards.

In making the recommendations above, it is noted that it is not possible to separate provisions for NIS from general provisions for cyber security which have been developed by a broad array of ICT standards bodies and implemented to varying extents by the entities subject to the NIS Directive. A significant concern consists in the fact that EU Regulation No 1025/2012 referenced by the NIS Directive only defines a small handful of organisations as constituting standardization bodies. This is not an accurate reflection of the current state of the market, nor those used within the highly specialized sectors to which the Directive applies.

Furthermore, NII, NIS and Cyber security cannot be geographically isolated and applied only to the European Union. This distributed complexity should be considered in implementing of the necessary information sharing required for effective NIS. Thus many of the capabilities of the NII, of commercial necessity, will be implemented using software and hardware from a global market and not a market restricted to the EU.

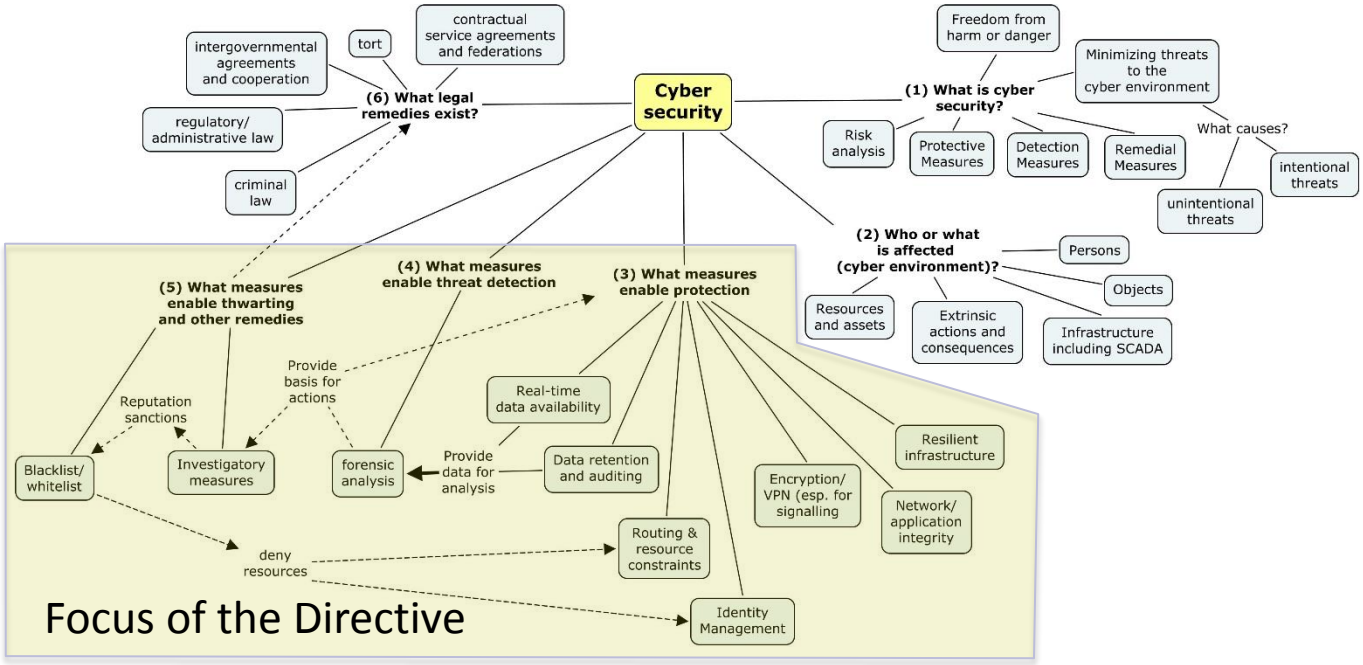
1. Landscape of the European NIS-related standardisation

1.1 The context for NIS

The Network Information Security (NIS) domain is one of the many dimensions of the multi-dimensional cyber-security landscape that can be visualised as a set of linked questions:

1. What is cyber security?
2. Who or what is affected? i.e. What is the cyber environment?
3. What measures enable protection?
4. What measures enable threat detection?
5. What measures enable thwarting and other remedies?
6. What legal remedies exist?

The NIS scope and the scope of what is cyber-security have considerable overlap and whilst the focus of the NIS Directive may be considered as relating to questions 3, 4 and 5 the reality is that the entire set of 6 questions needs to be considered in giving an assurance of NIS as required through the detail to be found in the articles of the NIS Directive. The visual model of the scope of the NIS Directive within Cyber-Security



is shown in Figure 1.

Figure 1: Visualisation of the relationship of NIS Directive to Cyber-security

Defense against attack of Network Information Systems shares the same set of fundamental building blocks as any other system. The well-known CIA paradigm (Confidentiality, Integrity, Availability) leads to well-known and understood triples of {threat, security-dimension, countermeasure} such as {interception, confidentiality, encryption}. The role of the CIA paradigm is most often seen in 2 areas: Risk analysis; and, Countermeasure deployment. The CIA paradigm applies equally to NIS as to any other domain in cyber-security.

1.2 European and global efforts in NIS standardisation

Standards are developed for global markets, and whilst there are some regional localisations that are addressed by the European Standardisation Organisations (ESOs) designated in Regulation (EU) No 1025/2012, the state of the global standards market in the NIS and Cyber-security domain is complex and highly specialized within ICT sectors. Practically the formal recognition processes for technical standardisation has been progressively side-lined by the rapid growth over the past twenty years of what may be termed alternative standards development bodies.

The following list enumerates the bodies involved in global cyber security standards whilst a more complete list of bodies is maintained by ETSI in ETSI TR 103 306 and a similar list has been captured in report number 3 of the Cyber Security Focus Group (CSCG).

3GPP	CCRA	ETSI ISI	IIC	OAA	Platform Industrie 4.0
3GPP SA2	CEN	ETSI LI	InfluxDB	OASIS	RIOT
3GPP SA3	CENELEC	ETSI MTS-SIG	IO-Link	OASIS CTI	ROS
3GPP SA5	CEPOL	ETSI NFV	IoT Security Foundation	ODVA	SAE International
3GPP CT	CERT-EU	ETSI NTECH	IoTivity	OGC	SensiNact
ACDC	CIA	ETSI SAGE	IPEN	OIC-CERT	SGIP
ACEA:	CIIAII	FIDO Alliance	IPSO	OM2M	Sofia2
AEF	CIS	FIRST	ISA	OMA	TCG
AIOTI	CLEPA	Fi-ware	ISF	OMG	The KNX Association
AllJoyn	Contiki	GlobalPlatform	ISO	OneM2M	The Open Group
Allseen Alliance	Continua: Health Alliance	GSMA	ISO JTC1/SC27	ONOS	The ULE Alliance
Apache Spark	CSA	GSMA FASG	ISO JTC1/SC6	OPC Foundation	The ZigBee Alliance
APCERT	CSC	H2020	ISO JTC1/SC7	Open Connectivity Forum	ThingSpeak
Arduino:	CSCG	HGI	ITU ITU-D	OpenDaylight	Thread group
ASHRAE	DICOM	HL7 International	ITU ITU-R	openHAB	TMForum
Automation ML	easyway	HYPER/CAT	ITU ITU-T	OpenIoT	UDG Alliance
AVNU	eCl@ss	ICANN	ITU	OpenRemote	UniverSaal
BEREC	EclipseIoT	IEC	LinuxIoTDM	OpenStack	UPnP
Bluetooth	ECRG	IEEE	LoRa Alliance	OpenWSN	W3C
Broadband Forum	ENISA	IEEE 802 LAN/MAN Standards Committee	MITRE	OPFNV	Weightless
C2C-CC	Enocean Alliance	IEEE P2413	Mosquitto	OSCE	Wi-Fi Alliance
CA/B Forum	ERTICO - ITS Europe	IETF	NATO	OSGi Alliance	WWRF
Cable Labs	ETSI	IETF IRTF	NATO CCDCOE	OWASP	
Calypso	ETSI CYBER	IETF MILE	NATO LIBGUIDE	Paho	
CCC	ETSI E2NA	IETF SACM	NIST	Particle	
CC-Link	ETSI ESI	IHE	Node-RED	PI International	

Table 1: Significant Cyber Security Standards fora

The actual global cyber security standards ecosystem today used by the ICT industry is depicted in Table 1. This ecosystem is, however, so complex and rapidly evolving that it is probably incomplete. The Table

reflects the recognition in Recital (32) of the NIS Directive that “standardisation of security requirements is a market-driven process.”

Unfortunately, the definition of what constitutes a standard or a specification in the Directive is fundamentally at odds with this recognition by referencing Regulation (EU) No 1025/2012 which excludes almost all the bodies cited in Table 1. (Only CEN, CENELEC, ETSI, ISO/IEC and ITU are recognized as standards bodies).

An immediate consequence of the diversity of the current standardisation ecosystem, and because of the extremely rapid pace of change, is that it is increasingly difficult to authoritatively determine if gaps in standardization or in capability exist. Any failure to recognize the reality of the ecosystem and the constituent members will gravely harm the aims of the NIS Directive and the harmonization of NII/NIS.

1.2.1 Critical Infrastructure Protection initiative support to NIS

The ERNCIP (European Reference Network for Critical Infrastructure Protection) initiative has identified a set of Cyber Security and Network protection standards. However, the ERNCIP work has not addressed NII as a domain in its own right and this needs to be revised. The NII is increasingly a component of all other Critical Infrastructures and this trend is expected to continue to the point that all CI shall have an NII component.

1.3 Work of Cybersecurity Focus Group (CSCG)

Within the EU the core standards bodies (CEN, CENELEC and ETSI) have set up the Cybersecurity Coordination Group (CSCG), transformed into Cybersecurity Focus Group (keeping the same acronym) after withdrawal of ETSI, which main goals include giving strategic advice to the technical committees of European standards developing organisations and EU Institution. In this frame, the CSCG has undertaken extended work emanating from the White Paper "*Recommendations for a Strategy on European Cyber Security Standardisation*" resulting in a further set of documents aimed at defining the term Cyber Security and the stakeholders involved. As noted above, it is not possible to distinguish capabilities for NII/NIS from the provisions for the general ICT/Cybersecurity domains and thus many of the recommendations of the CSCG apply equally to NIS.

1.4 New context – NIS Directive

Whilst it may be suggested that the NIS Directive imposes new requirements, it is probably more correct to state that the NIS Directive imposes essential requirements for harmonization and interoperability of the attack and defense context. The illustration in Figure 2 identifies the interfaces and operations to be made common for NIS Directive conformance.

- NOTE 1: Each Member State will designate one or more CSIRTs. If multiple, the Competent Authority will coordinate
- NOTE 2: Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC; processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001 [Article 1a]

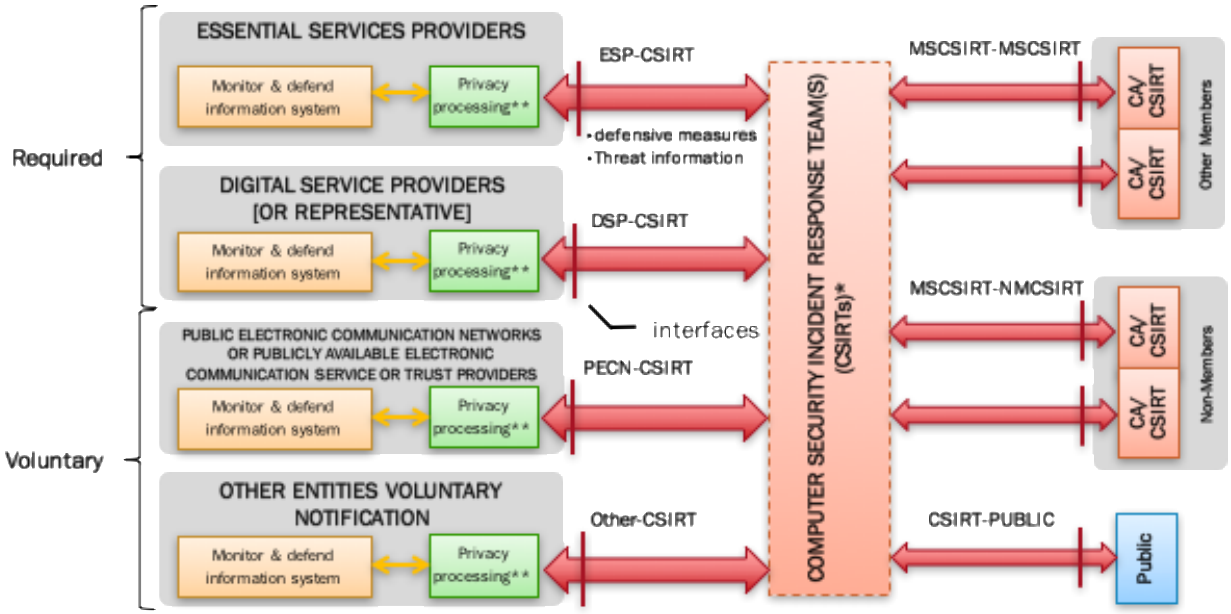


Figure 2: Interfaces of NIS Directive

As indicated in Table 1, above, there are many bodies proposing standardisation in these areas. The key aspects identified in the NIS Directive are those dealing, as shown in Figure 2, with reporting between a service provider and the CSIRT (variously named as ESP-CSIRT, DSP-CSIRT, PECN-CSIRT, and other-CSIRT) and between the CSIRTs and the Competent Authorities.

Internally to the service provider domain are two key sets of actions to be undertaken:

- Monitor and defence of the information system
- Privacy compliance processing

2. Analysis of the NIS Directive against standards requirements

This document provides an analysis of gaps in the standards landscape for Network and Information Security and provides recommendations for further standards development to allow the NIS Directive to be fulfilled and for the wider domain of NII to give assurances of security. An article by article summary of the analysis is given in "Annex B: Summary of NIS Directive technical requirements".

The analysis of gaps and subsequent recommendations are derived from an analysis of the NIS Directive to identify where standards are explicitly called for or are mentioned as requirements.

The research, however extends beyond the core standardisation requirements of the NIS Directive, but takes into account other areas mentioned in the directive, where standards might be considered helpful, but also reviews where requirements from other areas may potentially overlap or even contradict requirements exposed by the NIS Directive.

The analysis of requirements has been mapped against existing standards to identify if such existing standards may form the basis of a NIS framework.

Where possible, draft standards and projects at earlier stages have been considered. This is particularly important as the NII and general networking world are continuously evolving and the role of network virtualization, of the greater use of cryptography, and of the evolution in the role of virtual operators of networks and services, has been taken into account in identifying the broad set of requirements for NIS.

In line with the objectives of the NIS Directive, a strong focus was given to generic process-oriented standards for cyber security in organizations (risk management, information sharing, etc.). Conversely, cybersecurity standards in NIS Directive Art. 14 essential services sectors (energy, transport, banking, financial markets, etc) were not significantly examined. In other cases, such as NIS Directive Art. 15 Digital Services (cloud computing, IoT, embedded systems, big data, etc.), dedicated cyber security standards (e.g. public key infrastructure) were taken into account. The highly disparate sectors made it infeasible to take into account all the standards in a comprehensive fashion within a single focused analysis.

Within the recommendations, attention was given to the existing initiatives that could benefit from synergies with work in standards, especially involving contractual Public-Private Partnerships (cPPPs) and Horizon 2020 (H2020).

3. NIS Directive requirements

3.1 Overview

As a result of performed deconstruction of NIS Directive, several distinct areas have been identified, where specific requirements can be reflected in standards. A more in depth review is given below that expands upon the article-by-article review of Annex B.

3.2 Risk management for networks and information systems

Articles 14 and 15 of the NISD require “appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems” for operators of essential services and digital service providers respectively. With regards to the latter, the NISD specifically requires to take into account:

- security of systems and facilities,
- incident management,
- business continuity management,
- monitoring, auditing and testing,
- compliance with international standards.

Recent activity in ETSI has led to the publication of ETSI TR 103 305 addressing the role of ICT in Critical Infrastructure. It contains detailed consideration of the role of business continuity management, risk analysis and incident management. Whilst ETSI, in its Technical Committee CYBER, has committed to the extension of this work, there is still no formal plan in place to accomplish this task. Some work has also been done in ISO/IEC JTC1 SC27, which addresses risk and security management in the ISO 27000 series of management documents.

Furthermore, ETSI has published a modified set of controls for cyber security. In a similar fashion to the ICT for CI work, they will be further refined in normative specifications in due course. Additional work that addresses event detection within the context of risk analysis and incident management can be found in the following specifications:

- ETSI GS ISI 004 V1.1.1 (2013-12): Information Security Indicators (ISI); Guidelines for event detection implementation
- ETSI GS ISI 002 V1.2.1 (2015-11): Information Security Indicators (ISI); Event Model A security event classification model and taxonomy

As part of the rapid evolution and extension of the existing specifications for Structured Threat Information Expression (STIX), Trusted Automated eXchange of Indicator Information (TAXII) and Cyber Observable eXpression (CybOX) within the OASIS (standardisation body with which ETSI cooperates closely), additional risk and event categorizations are being added.

3.3 Impact prevention and minimisation

As noted, Articles 14 and 15 of the NISD require appropriate technical and operational measures "to prevent and minimise the impact of incidents affecting the security of the networks and information systems" for operators of essential services and digital service providers respectively. The Critical Security Controls specified in TR 103 305 are especially relevant, and efforts are underway to adjust the controls very quickly in response to threat conditions. The topic of risk management is also addressed by ETSI in TS

102 165-1 and ISO/IEC 15408 in the context of security assurance, as well as by some of the ISO/IEC JTC1 27000 series of specifications.

There is a significant issue arising from impact prevention, surrounding recovery to an equivalent stable state. This has been addressed in ETSI TR 103 303 with a summary of the concern stated as follows: "If an attacker has exploited systems using "strategy A" which have been successfully immunised against, it is essential that all connected and stakeholder systems that are vulnerable to the same "strategy A" have to be similarly immunised in order to defend against future attacks where "strategy A" is used as a side-channel attack at a related stakeholder". The reporting of an attack and the means used to immunize the system thus have to be shared, in order to prevent the form of side channel attack indicated.

3.4 Computer Security Incident Response Teams (CSIRTs), Competent Authorities, and Single Points of Contact

In Article 7, the NISD requires Member States to designate one or more Computer Security Incident Response Teams (CSIRTs) "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." Where there are multiple CSIRTs, a Competent Authority within the Member State and a designated Single Point of Contact are also key entities that are part of the structured exchange of information. Annex I further provides an extensive list of required capabilities, such as:

- high availability of communications services by avoiding single points of failure and providing several means for being contacted and for contacting others at all times
- communication channels clearly specified and well known to the constituency and cooperative partners.
- appropriate system for managing and routing requests, in order to facilitate handovers
- infrastructure whose continuity of operation is ensured

The complete set of entities and associated information exchange architecture resulting from Art. 7 is very complex – as depicted in Figure 2, above. Not only can there be multiple entities within each Member State, among whom information must be exchanged, but there are also equivalent entities in every other Member and Non-Member State that have to be accommodated. It is also foreseeable that some Member States for highly specialized Essential Services will designate third party entities collectively representing the operators (e.g., Information Sharing and Analysis Centres). In addition, foreign providers of digital services must designate domestic representatives for purpose of the NISD requirements.

3.5 Identification of Operators

Article 3a (5) of the NISD requires the Cooperation Group to support a consistent approach among Member States to identify (cf. lit. a-d) operators of essential services.

In identifying NII as a component of CI, the guidance of ETSI TR 103 303 and succeeding work should be considered as the base for future standardization. In particular, ETSI TR 103 303 recommends that organisations should be familiar with the definition(s) of CI in their sector(s) and the government body acting as a point of contact in this area. Any organisation believing that they either meet the relevant definition of CI or will do so in the near future should notify the relevant government body. In the context of NISD, the Competent Authority for NIS may also be considered as the Competent Authority for CI.

4. Recommendations

The NISD analysis given in Annex B has identified a small number of gaps in standardisation and some areas of overlap where there is no clear best practice to be adopted. The standardisation analysis has considered a very much wider spectrum of Standards Development Organisations (SDOs) than is implied by the text of Article 16 of the NSID which refers to "internationally accepted standards". The interpretation of this Article for the purpose of presented analysis has been to include standards that have acceptance in the industry from a wide set of bodies. This includes those established under Regulation (EU) No 1025/2012, but should be also extended to the recognised de-facto and industrial groups, thus including groups such as IETF, W3C, OASIS, and established national bodies with international recognition, like FIPS, NIST, BSI and others. A list of such standards bodies with particular roles in Cyber Security, and by inference in Network Information Security, has been published recently as ETSI TR 103 306. It is strongly recommended that this source is adopted as a list of bodies preparing "internationally accepted standards". It is further noted that this list has been summarised in the Cybersecurity Focus Group (CSCG) report number 3 and is presented in Table 1 of this document.

The immediate priority is to simplify the standards for NIS that enable interoperability of event reporting and information sharing. The controls for cyber security have been transposed for the EU context in ETSI TR 103 305. Specific recommendations include:

- Reach consensus among Member States and major partners on
  - Architectures, interfaces, and information exchange expressions
  - Standards and specifications
- Given the strong similarities of the NIS Directive and USA Cybersecurity Act, the two implementations should be harmonized to the extent possible, including common architectures, interfaces, structured information expressions and privacy filters
- Develop a means for Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) to fit into the NIS Directive model and architecture
- Develop means for Public Electronic Communication Networks or Publicly Available Electronic Communication Service Providers under EU Directive 2002/21/EC and Trust Providers to fit into the NIS Directive model and architecture
- Develop additional border gateway defence and threat exchange standards for one Essential Service (Digital Infrastructure Internet Exchange Points)
- Develop a means for NFV, SDN, MEC and other virtualised infrastructures and services to fit into the NIS Directive model and architecture

Annex A: Definitions and abbreviations

A.1 Definitions

The following definitions from the NIS Directive apply in the present document:

- **Network and information system**: (a) an electronic communications network within the meaning of Directive 2002/21/EC, and (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as (c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.
- **Security**: The ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;
- **Risk**: any circumstance or event having a potential adverse effect on security;
- **Incident**: any circumstance or event having an actual adverse effect on security;
- **information society service**: service within the meaning of point (2) of Article 1 of Directive 98/34/EC;
- **NIS cooperation plan**: a plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of a risk or an incident affecting them;
- **incident handling**: all procedures supporting the analysis, containment and response to an incident;
- **market operator**: (a) provider of information society services which enable the provision of other information society services, a non-exhaustive list of which is set out in Annex II of the NIS Directive; (b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non-exhaustive list of which is set out in Annex II of the NIS directive.
- **Standard**: a standard referred to in Regulation (EU) No 1025/2012;
- **Specification**: a specification referred to in Regulation (EU) No 1025/2012;
- **Trust service provider**: a natural or legal person who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.

A.2 Abbreviations

- **ENISA**: European Union Agency for Network and Information Security
- **ETSI**: European Telecommunications Standards Institute
- **NISD**: Network and Information Security Directive

Annex B: Summary of NIS Directive technical requirements

B.1 Overview

Below is the set of stakeholders identified in the NIS Directive:

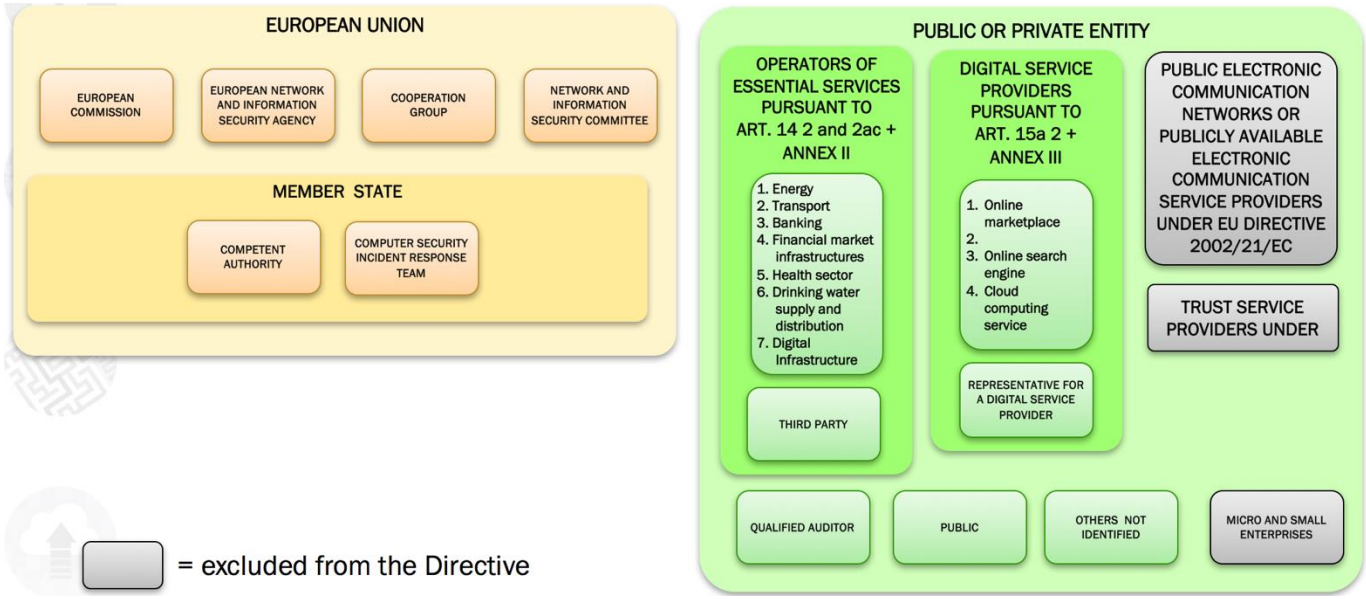


Figure 3: Stakeholders of NIS Directive

Basing on the Figure 3, we can identify sets of responsibilities of each stakeholder in the NIS Directive (by article):

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
4	Member States	Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive	None	The term "high level of security" is undefinable. The affected systems are assumed to be those identified that support essential services.
5	Member States	Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security.	See table in Annex C on national regulatory measures	Not a technical standards issue
6	Member States	[*The member states shall appoint a*] National competent authority on the security of network and information systems	None	Not a technical standards issue

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
7	Member States	Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") 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 CERT may be established within the competent authority	The ENISA report has cited 53 information sharing standards and 16 information management tools relevant to the concept of actionable information. The broad recommendation is to move towards STIX/TAXII/CyBOX for this domain.	Procedures for CERTs to interoperate are defined in general terms. Many EU MS have already identified their CERTs. ENISA has prepared reports on the general topic of data exchange but as noted they cite large numbers of standards and practices with no single harmonised specification. The number of cited standards is of itself a problem and pending a more detailed analysis it is highly likely that the overall picture leads to confusion and overlap. It is suggested that an initial response is a best practice guide that identifies specific standards for specific actions and that overall the number of citations is cut to the single best practice document to be agreed by all MS.

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
8	Competent authorities, European Commission	To form a *permanent* network ("cooperation network") to cooperate against risks and incidents affecting network and information system	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	This article stipulates: "*The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2)*" which may imply standards need to be developed and cited
9	Competent authorities, European Commission	The "cooperation network" to be intrinsically secure	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	Implementing acts may be required

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
10	Competent authorities, European Commission	To use the "cooperation network" to exchange information of the form "early warning"	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	Delegated acts may be required
11	Competent authorities, European Commission	To give assurance based on information from the early warnings received via the "cooperation network" of a coordinated response	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER). The impact here extends to working practice and policy and not to technical specifications.	Responses will be made at national level and coordinated but the cooperation model needs policy development.
12	European Commission	To adopt, by means of implementing acts, a Union NIS cooperation plan	Extends the technical and policy framework from articles 7 through 12.	Policy not technical.

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
13	European Union	Shall allow for harmonised international cooperation	This may be more easily fostered if the programme of standards supporting the "cooperation network" are also in common use internationally	Adopting the STIX/TAXII/CyBOX approach in close cooperation with international partners may achieve this goal more easily, notwithstanding the political issues that may need to be negotiated.
14	Competent authorities, Member States, Market operators, Public Administration	To deploy risk managed secure networks and infrastructure	The standards track identified by the EU ERNCIP programme applies with additional attention paid to specific controls under the ISO 27000 family of management standards.	ISO 27001 in particular is not very precise and has a cost burden to implement for SMEs who although excluded for now from the NISD may be in the overall supply chain and this requires that the entities they supply to take responsibility for all entities in the supply chain

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
15	Member states, Competent authorities	Powers to enforce compliance and investigate non-compliance	The suggestion is that market operators need to prove the security of their networks. This could imply Common Criteria (recommended) or some other assurance scheme. Current standards do apply including ISO/IEC 15408 and NIST SP 800	Target of what is to be complied to needs to be stated. This should be a stated NIS Protection Profile or close equivalent.
16	Member States	Encourage implementation of article 14 by use of implementing acts	As noted there are a number of existing standards to undertake risk analysis and the sharing of the results of such analysis.	The notes from Article 14 apply
17	Member States	Harmonised sanctions for failure to implement	None	Not a technical standards issue but requires harmonisation of sanctions. It is noted that attacks may arise from outside the EU and other international laws may need to be invoked
18	Member States	Power to adopt delegated acts	None	Not a technical standards issue
19	European	To establish a NIS Committee	None	Not a technical standards issue
20	European Commission	To establish a review process	None	Not a technical standards issue

Article number	Affected stakeholder	Responsibility	Reference standard	Observations
21	Member States	Transposition of NISD to provisions in national law	None	Not a technical standards issue
22	Member States	To establish NISD as national law within 20 days of publication of NISD in official journal	None	Not a technical standards issue. However compliance without a sound standards basis may be difficult to enforce
23	Member States	Intended audience of NISD	None	Not a technical standards issue

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

Catalogue Number TP-06-16-337-EN-N

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

ISBN: 978-92-9204-186-1
DOI: 10.2824/975760