Cyber-Security in Europe:
The European Network and Information Systems (NIS) Security Directive

April 2017
MR - 198

Summary

The European Network and Information Systems (NIS) Security Directive sets a minimum baseline of requirements to ensure better protection of critical infrastructures in Europe. The legislation targets three broad groups of stakeholders. First, it looks first at Member States and sets basic principles for common minimum capacity building and strategic cooperation among others. The legislation also looks at operators of essential services (OES) and digital service providers (DSP) and directs them to ensure they apply basic common security requirements. NIS systems are considered to be the e-communications network, connected devices and digital data.

This Directive has been adopted by the EU in July 2016, at which point Member States have until May 2018 to transpose the Directive into their national legal framework.

Market opportunity:
The new obligations to both Member States and OES/DPS create market opportunities for U.S. solution providers. Member States are expected to equip themselves with both technical and organizational capabilities to prevent, detect, respond to and mitigate incidents and risks. OES/DSP in scope must match new requirements in the areas of security of systems and facilities; incident handling; business continuity management; monitoring, auditing and testing.

The full text of the NIS Directive can be found here: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

I. Who is covered by the NIS Directive?

The Directive addresses three broad groups of stakeholders:

1. The Member States: the Directive creates a number of action items for them, including an obligation to identify operators of essential services (OES);
2. operators of essential services (OES) identified by Member States;
3. digital service providers (DSP);

For stakeholders falling in categories 2 and 3, the Directive creates a set of security and notification requirements.

Other important stakeholders are:

- national competent authorities (e.g. the National Agency for the Security of Information Systems (ANSSI) in France, the Federal Office for Information Security (BSI) in Germany, the Information System Authority in Estonia) ;

- the European Union Agency for Network and Information Security (ENISA), for guidelines on specific issues.

1. Operators of essential services (OES):

Annex II lists the sectors of essential services to be covered by the Directive:
- energy (supply, distribution) for electricity, oil and gas;
- transport (traffic management bodies, infrastructure managers) for air, rail, water and road;
- banking (credit institutions),
- financial market infrastructures,
- healthcare (including hospitals and private clinics);
- drinking water supply and distribution,
- and digital infrastructures (i.e. Internet exchange points, domain name system service providers, top level domain name registries).

Sector-specific remarks:
In the water transport sector, security requirements (reporting of all incidents) for companies, ships, port facilities, ports and vessel traffic services cover all operations, including radio and tele-communication systems, computer systems and networks.

Banking and financial market infrastructures: the existing requirements often exceed the NIS Directive requirements. For instance requirements for notification of incidents are already part of normal supervisory practice in the financial sector.

2. Digital Service Providers (DSP):

The Directive applies to DSPs which are broadly defined to include:
- online/e-commerce marketplace (that definition does not cover price comparison tools but does include app stores).
- online search engine (with the exclusion of search function limited to a specific website);
- and Cloud computing service (i.e. scalable resources such as networks, servers or other infrastructure, storage, applications and services).

The following DSPs are exempted from the NIS Directive:
- social networks, price comparison tools;
- public communication networks providers or publicly available electronic communication services providers (because they are already covered by the "e-privacy" Directive 2002/58 for specific security and integrity requirements);
- trust service providers (because their specific notification requirements are laid down in Regulation 910/2014 on e-identification and trust services, in particular article 19);
- micro- and small enterprises;

II. What does it mean for DSP and OES?

A DSP and an OES are expected to ensure "the ability of NIS to resist any action that could compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those systems" (article 4(2)).

1. Obligations for an OES

The Directive creates the following obligations for OES:

- take appropriate and proportionate technical and organizational measures to NIS risk management;
- take appropriate measures to prevent and minimize the impact of NIS security incidents;
- notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact (including cross-border significance) on the continuity of the essential services they provide.

2. Obligations for DSP

- take appropriate and proportionate technical and organizational measures to ensure risk management of their NIS services;
- take measures to prevent and minimize the impact of incidents affecting their NIS security;
- notify, without undue delay, the competent authority or the CSIRT of incidents having a substantial impact (including cross-border significance) on the continuity of the essential services they provide
- (for DSP not based in the EU but servicing EU customers) designate a representative to be based in a Member States. The DSP will be under the jurisdiction of that Member State.

Cloud service providers to public administration may be submitted to additional security measures through contractual obligations. That determination is left to the Member States discretion.

The Directive allows competent authorities to exercise *ex post* supervisory measures if they have evidence that a DSP does not meet the security and notification requirements.

DSP can refer to this ENISA report for preliminary guidelines on incident notification. These guidelines do not however constitute binding requirements in the eyes of Member States: https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

3. Common remarks for both OES and DSP

The level of security expected from OES should be higher than the level expected from DSP, because of the degree of risk posed to their infrastructure.

The security and notification requirements apply to OES and DSP regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

The criteria for defining the significance of the incident are broadly defined by the Directive but are left to Member States' interpretation. They include: the number of users affected, the duration of the incident, its geographical spread (and for DSP its impact on economic and societal activities).

Incident notification requirements should not increase liability of the OES (article 14). However this is notwithstanding additional liability under the new data protection regulation (the General Data Protection Regulation or GDPR), should the incident include a personal data breach.

Member States may choose (or require the DSP) to inform the public about individual DSP or OES incidents in order to prevent/deal with the incident or if it is in the public interest. They should balance the interest of the public in being informed about threats against possible reputational and commercial damage.

4. Standardization

Cyber-Security: The European Network and Information Systems (NIS) Security Directive With a focus on security/notifications requirements and their enforcement, the Directive calls for Member States to promote technology-neutral European or internationally accepted standards and/or specifications on NIS Security. It is the role of the European Union Agency for Network and Information Security (ENISA) to advise Member States in the process, including regarding existing standards.

Note: On 12 February 2014, the National Institute of Standards and Technology steered the development of the Cybersecurity Framework as a voluntary, industry-driven reference document to help organizations with cybersecurity activities and risk management processes. There are three parts to the Framework: the Core, Profile, and Implementation Tiers. The Framework Core is a set of cybersecurity references, best practices and global standards and provides guidance for developing individual organizational Profiles for risk management. Through use of the Profiles, the organization will be able to align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. While the NIST Framework is not universally applied in Europe, it gives a useful frame of reference. Note that Italy has fully incorporated the NIST Framework.

5. Guidelines

The Directive mandates ENISA to develop guidelines. The following guiding documents have currently been released:

- Risk management: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management
- Incident notification for DSPs https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive.

III. Obligations for Member States

The text creates a series of obligations for Member States:

- adopt a **national NIS strategy** (including a governance framework, measures of preparedness, response and recovery, and a risk assessment plan);
- create one or more **CSIRTs** and join a Member States network for information sharing and voluntary mutual assistance; the CSIRTs should be able to receive notifications of incidents;
- designate **national competent authority**(ies) and/or a single point of contact to act as a liaison for cross-border cooperation;
- **identify** operators of essential services (OES) and establishes security and notification requirements for OES and for digital service providers (DSP);

- and create a "**cooperation group**" among Member States, with the European Commission (executive branch) and the participation of the European NIS agency (ENISA) to provide guidance to the CSIRTs network, exchange best practices and exchange information; this group could be a venue for international cooperation.

IV. Timeline for implementation

The Directive has to be transposed by Member States. After its entry into force (August 2016), Member States are expected to match the following deadlines for implementation:

Date	entry into force + ...	Milestone
August 2016	-	Entry into force
February 2017	6 months	Cooperation Group begins tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
May 2018	21 months	Transposition into national law
November 2018	27 months	Member States to identify operators of essential services
May 2019	33 months (i.e. 1 year after transposition)	Commission report assessing the consistency of Member States' identification of operators of essential services
May 2021	57 months (i.e. 3 years after transposition)	Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers

Source: European Commission: http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

V. More information:

European Commission webpage on the NIS Directive:
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Union Agency for Network and Information Security website:
https://www.enisa.europa.eu/

Directive 2002/58 "e-privacy" (full text):
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN. Note: a review of the Directive 2002/58 was proposed by the European Commission in January 2017.

Regulation 910/2014 on e-identification and trust services (full text):
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&qid=1491493738191&from=EN

General Data Protection Regulation - GDPR (full text): http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

NIST Cyber Framework: https://www.nist.gov/cyberframework

CSIRTs by Country - Interactive Map: https://www.enisa.europa.eu/topics/national-csirt-network/csirt-inventory/certs-by-country-interactive-map

***

For More Information:
The U.S. Commercial Service at the U.S. Mission to the European Union is located at Boulevard du Regent 27, Brussels 1000, Belgium, and can be contacted at +32 2 811 4817. See also: www.export.gov/europeanunion.

The U.S. Commercial Service — Your Global Business Partner

With its network of offices across the United States and in more than 80 countries, the U.S. Commercial Service of the U.S. Department of Commerce utilizes its global presence and international marketing expertise to help U.S. companies sell their products and services worldwide. Locate the U.S. Commercial Service trade specialist in the U.S. nearest you by visiting http://www.export.gov/.

To the best of our knowledge, the information contained in this report is accurate as of the date published. However, the Department of Commerce does not take responsibility for actions readers may take based on the information contained herein. Readers should always conduct their own due diligence before entering into business ventures or other commercial arrangements. The Department of Commerce can assist companies in these endeavors.

INTERNATIONAL COPYRIGHT, U.S. DEPARTMENT OF COMMERCE, 2011. ALL RIGHTS RESERVED OUTSIDE OF THE UNITED STATES.