Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity

The NIS Directive is the first EU-wide legislation on cybersecurity. The objective of the Directive is to achieve evenly high level of security of network and information systems across the EU, through:

1. Improved cybersecurity capabilities at national level;
2. Increased EU-level cooperation;
3. Risk management and incident reporting obligations for operators of essential services and digital service providers.

As part of the cybersecurity package adopted in September 2017, the Commission issued the Communication "Making the Most of the Directive on Security of Network and Information Systems" to assist Member States with guidance and best practice examples as well as to ensure a harmonised transposition of the new rules.

According to the Directive, all Member States need to adopt a **national strategy on the security of network and information systems** (NIS Strategy) defining the objectives and appropriate policy and regulatory measures. The strategy should include:

- Strategic objectives, priorities and governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Awareness raising, training and education
- Research and development plans related to NIS Strategy
- Risk assessment plan
- List of actors involved in the strategy implementation

Member States have to designate at least one **national competent authority** to monitor the application of the NIS Directive at national level and to nominate a **single point of contact** to liaise and ensure cross–border cooperation with other Member States. Additionally, the Member States need to appoint at least one **Computer Security Incident Response Team** (CSIRT). The CSIRTs role is to:

- monitor incidents at national level;
- provide early warning, alerts and information to relevant stakeholders about risks and incidents;
- respond to incidents;
- provide dynamic risk and incident analysis and increase situational awareness;
- participate in a network of the CSIRTs across Europe.

The European Commission supports Member States financially to increase their operational capabilities through the Connecting Europe Facility (CEF) – a key EU funding instrument for cross-border infrastructures in digital sectors. The CEF programme is providing €6.3 million in funding for the cooperation and information sharing platform for the Computer Security Incident Response Teams (CSIRTs), known as MeliCERTes. €18.7 million are allocated from the CEF programme for cybersecurity projects increasing capabilities of the CSIRTs between 2017 to 2020 (for example, for purchasing software tools, or covering the costs of trainings and exercises).

CEF funding is additionally being opened up to other stakeholders concerned by the NIS Directive – namely operators of essential services, digital service providers, single points of contact and national competent authorities with a further €13 million being available to those who apply under the next call for proposals from May to late November this year.

The NIS Directive established a **cooperation group that** is chaired by the Presidency of the Council of the European Union. The group gathers representatives of the Member States, the Commission (acting as secretariat) and the European Union Agency for Network and Information Security (ENISA). This cooperation group facilitates strategic cooperation and exchange of information among Member States and helps develop trust and confidence. The cooperation group has met six times to date starting from February 2017.

The Directive also established a **Network of the national Computer Security Incident Response Teams** (network of CSIRTs), to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

The group is chaired by a representative of the Member State holding the Presidency of the Council of the EU. It operates by consensus and can set up sub-groups to examine specific questions related to its work. The Commission provides the secretariat of the cooperation group.

The group works on the basis of **biennial work programmes**. Its main tasks are to steer the work of the Member States in the implementation of the Directive, by providing guidance to the Computer Security Incident Response Teams (CSIRTs) network and assisting Member States in capacity building, sharing information and best practices on key issues, such as risks, incidents and cyber awareness.

The Cooperation Group has so far produced, for example, non-binding guidelines on the security measures and the incident notification for operators of essential services.

Every one and a half years the group will provide a report assessing the benefits of the cooperation. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

How does the CSIRTs Network function?

The network is composed of representatives of the Member States' CSIRTs

(Computer Security Incident Response Teams) and CERT–EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). The Commission participates in the CSIRTs Network as an observer. The European Union Agency for Network and Information (ENISA) provides the secretariat, actively supporting the cooperation among the CSIRTs.

Two years after entry into force of the NIS Directive (by 9 August 2018), and every 18 months thereafter, the CSIRTs Network will produce a report assessing the benefits of operational cooperation, including conclusions and recommendations. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

More intense coordination in the netowork could be seen already mid-2017 during the Wannacry and Non-Petya ransonware attacks.

What are operators of essential services, and what will they be required to do?

Operators of essential services are private businesses or public entities with an important role to provide security in healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply.

Under the NIS Directive, identified operators of essential services will have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority.

The security measures include:

- Preventing risks
- Ensuring security of network and information systems
- Handling incidents

How will Member States identify operators of essential services?

Member States have until 9 November 2018 to identify the entities who have to take appropriate security measures and to notify significant incidents according to the following criteria criteria:

(1) The entity provides a service which is essential for the maintenance of critical societal and economic activities;

(2) The provision of that service depends on network and information systems; and

(3) A security incident would have significant disruptive effects on the essential service.

Which sectors does the Directive cover?

The Directive covers operators in the following sectors:

- Energy: electricity, oil and gas

- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare settings
- Water: drinking water supply and distribution
- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries

What kind of incidents should be notified by the operators of essential services?

The Directive does not define threshold of what is a significant incident requiring notification to the the relevant national authority. Three parameters that should be taken into account regarding the notifications are:

- the number of users affected;
- the duration of the incident;
- the geographic spread.

What are digital service providers and do they have to notify cyber incidents?

The NIS Directive covers:

- Online marketplaces (that allow businesses to make their products and services available online)
- Cloud computing services
- Search engines

All entities meeting the definitions will be automatically subject to the security and notification requirements under the NIS Directive. Micro and small enterprises (as defined in Commission Recommendation 2003/361/EC) do not fall under the scope of the Directive.

What are the obligations for digital service providers?

Digitial service providers covered by the NIS Directive are required to take appropriate security measures and to notify substantial incidents to the competent authority.

Security measures are similar to those undertaken by the operators of essential services and cover the following:

- Preventing risks
- Ensuring security of network and information systems
- Handling incidents

The security measures taken by digital service providers should also take into account some specific factors defined in the 2018 Commission implementing regulation:

- security of systems and facilities: a set of policies to manage the risk posed to the security of DSPs, which can be aimed at facilitating

technical IT security as well as physical and environmental security or the security of supply and access control;
- incident handling: measures taken to detect, report and respond to cybersecurity incidents and assess their root causes;
- business continuity management: the capacity to be adequately prepared with the ability of minimise impacts on services and to quickly recover from cyber incidents.
- monitoring, auditing and testing: regular checks to assess anomalies, verification that risk management measures are in place and that processes are being followed.
- compliance with international standards, for example, those adopted by international standardisation bodies (e.g. ISO standards).

What kind of incidents will be notifiable by the digital service providers?

The Directive defines five parameters that should be taken into consideraton, as specified by the Commission in its 2018 implementing regulation:

- Number of users affected: users with a contract in place (especially for online marketplaces and cloud computing service) or habitually using the service (based on previous traffic data);
- Duration of incident: the period of time starting when a digital service is disrupted until when it is recovered;
- Geographic spread: the area affected by the incident;
- The extent of the disruption of the service: characteristics of the service impaired by an incident;
- The impact on economic and societal activities: losses caused to users in relation to health, safety or damage to property.

The implementing regulation specifies four situations in which digital service providers are required to notify the relevant national competent authority or CSIRT, notably:

- If the digital service is unavailable for more than 5 million user-hours in the EU;
- If more than 100,000 users in the Union are impacted by a disruption;
- If the incident has created a risk to public safety, public security or of loss of life;
- If the incident has caused material damage of more than €1 million.

This list may be reviewed on the basis of guidance issued by the cooperation group, which will take into account the experience gained through the implementation of the NIS Directive.

What is the timeline for implementation of the Directive?

Member States have time until 9 November 2018 to identify businesses operating in their territory as “operators of essential services” – i.e. private businesses or public entities with an important role for the society and economy operating in critical sectors that will have to comply with security requirements and notify to national authorities significant incidents. The Commission will regularly update the overview on the state-of-

play of transposition in each Member State on its website.

For More Information

Joint statement by Vice-President Ansip and Commissioners Avramopoulos, King and Gabriel