Directive on Security of Network and Information Systems

Brussels, 6 July 2016

Questions and Answers

The European Parliament's plenary adopted today the Directive on Security of Network and Information Systems (see welcoming statement by European Commission Vice-President Andrus Ansip, responsible for the Digital Single Market, and Commissioner Günther H. Oettinger, in charge of the Digital Economy and Society).

The Directive on Security of Network and Information Systems ('NIS Directive') represents the first EU-wide rules on cybersecurity. The objective of the Directive is to achieve a high common level of security of network and information systems within the EU, by means of:

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

1. Improved cybersecurity capabilities at national level

What will Member States do to increase their national cybersecurity capabilities?

Each Member State will adopt a **national strategy on the security of network and information systems** defining the strategic 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 & development plans related to NIS Strategy
- Risk assessment plan
- List of actors involved in the strategy implementation

Member States will designate one or more **national competent authorities** for the NIS Directive, to monitor the application of the Directive at national level.

Member States will also designate a single point of contact, which will exercise a liaison function to ensure cross–border cooperation with the relevant authorities in other Member States and with the cooperation mechanisms created by the Directive itself.

Member States will designate one or more **Computer Security Incident Response Teams** (CSIRTs). CSIRTs will be responsible for, at least:

- monitoring incidents at a national level
- providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents
- responding to incidents
- providing dynamic risk and incident analysis and situational awareness
- participating in the network of the national CSIRTs (CSIRTs network)

2. Increased EU-level cooperation

How will Member States cooperate?

The NIS Directive establishes a **Cooperation Group**, to support and facilitate strategic cooperation

and the exchange of information among Member States and to develop trust and confidence.

It also establishes a **network of the national CSIRTs**, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

What will the Cooperation Group do?

The Cooperation Group will be composed of representatives of Member States, the Commission and ENISA (the European Union Agency for Network and Information Security), with the European Commission acting as secretariat. The procedural arrangements necessary for the functioning of the Cooperation Group will be adopted by the Commission through implementing acts.

The Cooperation Group will work on the basis of biennial Work Programmes, in four different areas:

Planning:

- Establish a Work Programme 18 months after entry into force (i.e. February 2018)
- Prepare a Work Programme every two years thereafter

Steering:

- Provide guidance for CSIRTs Network
- Assist Member States in NIS capacity building
- Support Member States in the identification of operators of essential services
- Discuss incident notification practices
- Discuss standards
- Engage with relevant EU institutions and bodies
- Evaluate national NIS strategies and CSIRTs (on voluntary basis)

Sharing information and best practices on:

- Risks
- Incidents
- Awareness-raising
- Training
- R&D

Reporting:

- Every 1.5 years provide a report assessing the experience gained with cooperation. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

What will the CSIRTs Network do?

The CSIRTs Network will be composed of representatives of the Member States' CSIRTs and CERT–i EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). The Commission will participate in the CSIRTs network as an observer. ENISA will provide the secretariat and actively support the cooperation among the CSIRTs.

The CSIRTs Network will have the following tasks:

- exchanging information on CSIRTs services, operations and cooperation capabilities
- exchanging and discussing information related to incidents (on request and voluntary)
- identifying a coordinated response to an incident (on request and voluntary)
- support cross-border incident handling (voluntary)
- exploring further forms of operational cooperation
- informing the Cooperation Group of its activities and requesting guidance
- discussing lessons learnt from NIS exercises
- discussing issues relating to an individual CSIRT (on request)
- issuing guidelines on operational cooperation

Two years after entry into force of the NIS Directive, and every 18 months thereafter, the CSIRTs Network will produce a report assessing the experience gained with 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.

3. Risk management and incident reporting obligations for operators of essential services and digital service providers

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 for the society and economy.

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

The security measures include:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

How will Member States identify operators of essential services?

Each Member State will identify the entities who have to take appropriate security measures and to notify significant incidents by applying these criteria:

(1) The entity provides a service which is essential for the maintance of critical societal/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 provision of the essential service.

Which sectors does the Directive cover?

The Directive will cover such 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 will be notifiable by the operators of essential services?

The Directive does not define threshold of what is an significant incident requiring notification to thethe relevant national authority. It defines 3 paramaters which should be taken into consideraton:

- Number of users affected
- Duration of incident
- Geographic spread

These parameters may be further clariefied by means of guidelines adopted by the national competent authorities acting together within the Cooperation Group.

What are digital service providers (DSPs), and what will they be required to do?

Important digital businesses, referred to in the Directive as "digital service providers" (DSPs), will also be required to take appropriate security measures and to notify substantial incidents to the competent authority.

Security measures cover the following:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.

- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

The security measures taken by DSPs should also take into account some specific factors, to be further specified in a Commission implementing act:

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

What kind of incidents will be notifiable by the DSPs?

The Directive does not define thresholds of what is a substantial incident requiring notification to thethe relevant national authority. It defines 5 paramaters which should be taken into consideration:

- Number of users affected
- Duration of incident
- Geographic spread
- The extent of the disruption of the service
- The impact on economic and sociatal activities

These parameters will be further specified by the Commission by means of implementing acts.

Which Digital Service Providers does the Directive cover?

The Directives covers:

- Online marketplaces (which allow businesses to set up shops on the marketplace in order 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.

How will a light-touch and harmonised approach for DSPs be achieved?

The Commission will adopt implementing acts with regard to security requirements and notifications obligations of DSPs within one year from the adoption of the Directive. Member States will not be able to impose additional more stringent security and notification requirements on DSPs. In addition, the competent authorities will be able to exercise supervisory activities only when provided with evidence that a DSP is not complying with its obligations under the Directive

What is the timeline for implementation of the Directive?

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