

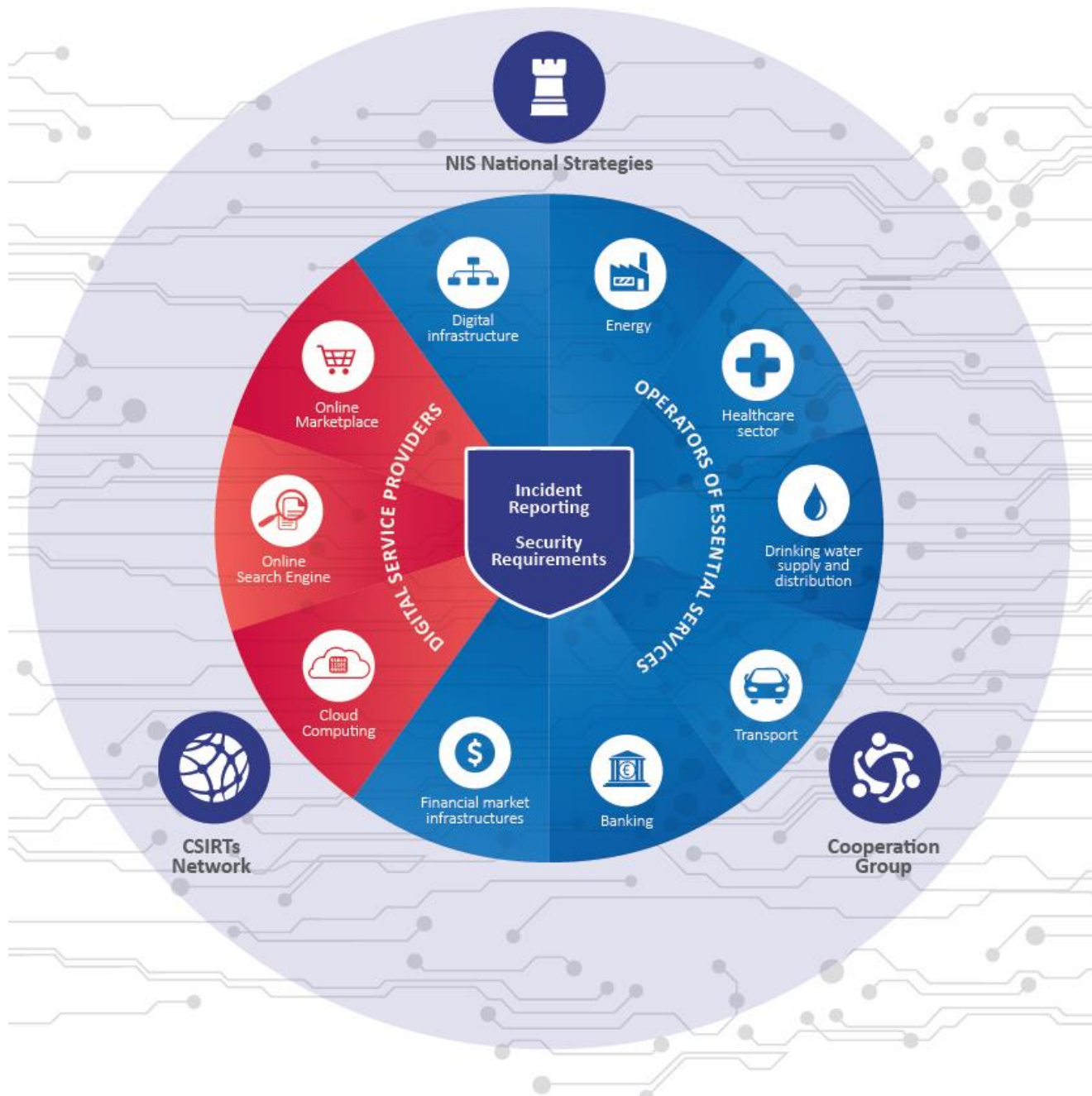
Network and Information Security Directive Provisions + ENISA's activities

Dr Evangelos Ouzounis

Head of Secure Infrastructure and Services Unit, ENISA

European Union Agency for Network and Information Security





The NIS Directive (EU 2016/1148)



Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

Status: ADOPTED August 2016.

Deadline for transposition: 9 May 2018 (21 months).

Provisions:

1. Improved cybersecurity capabilities at national level
2. Increased EU-level cooperation
3. Obligations for operators of essential services (OES)
4. Obligations for digital service providers (DSP)



1. Improved cybersecurity capabilities at national level



- adopt a national **NIS strategies** to include:
 - Strategic objectives, priorities and governance framework
 - Measures on preparedness, response and recovery
 - Cooperation methods between the public and private sectors
- designate one or more **national competent authorities**.
- designate one or more **Computer Security Incident Response Teams (CSIRTs)**:
 - Monitoring incidents national level
 - Providing early warning, alerts
 - Incident response



2. Increased EU-level cooperation



- Creates first EU **Cooperation Group** on NIS
 - Assist MS in NIS capacity building
 - Support MS in the identification of OES
 - Evaluate national NIS strategies and effectiveness of CSIRTs (on voluntary basis)
 - Provide strategic guidance for CSIRTs network
- Creates a **Network of National CSIRTs**
 - Exchange information
 - Provide support and identify forms of coordinated incident response for cross-border incident handling.



CSIRTs network



- **Article 9 and 12** of the Directive gives the framework for CSIRTs
 - **Why (paragraph 1):**
 - Develop confidence and trust between Member States
 - Promote swift and effective operational cooperation
 - **Composition (paragraph 2):**
 - representatives of the Member States' CSIRTs
 - CERT-EU (CSIRT for EU institutions)
 - ENISA (secretariat and active support)
 - European Commission (as observer)
 - **Tasks (paragraph 3):**
 - Exactly how the group will perform its 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.
- **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

3. Obligations for MSs on OES



- Identification of operators of essential services.
- Minimum security measures to ensure a level of security appropriate to the risks.
- Incident notification to prevent and minimize the impact of incidents on the IT systems that provide services.
- Make sure authorities have the powers and means to assess security and check evidence of compliance for OES.



Challenges for the transport sector



- Interdependencies
- Cross border services
- Intermodality
- Overlapping regulations
- Lack of security standards for the different transport modes
- Existing incident notification schemes for safety
- Different authorities
- Emerging technologies

ENISA's role to support MS with OESs



In 2017 ENISA assists MS

- Identification of OES
 - Preliminary work started in 2016, namely by:
 - looking into approaches taken by MS in identifying OES;
- Minimum Security Measures for OES
 - Cross sector security measures
 - Mapping with well known standards for all sectors
- Incident reporting guidelines for OES

CSIRTS Network - Status



- **2 formal meetings in 2017 and 3 informal ones in 2016**
 - last meeting Oct 2017 in Heraklion
- **Working Groups**
 - SOPs for CSIRTS
 - Security Requirements for Services
 - Building Functional exchange with Coop. Group
 - CSIRTS maturity assessment and CSIRTS network portal development
- **Coordination and Synergies with CEF/CSP project and CEF call for proposal for CSIRTS**

Key success factors

- Build trust amongst the members of the CG and the CSIRTs network
- Enhanced engagement by the MSs
- Active support with facilitation, surveys and stock takings and reports
- Assist MS in the implementation of the NIS Directive



NIS directive - TIMELINE



August 2016	-	Entry into force
February 2017	6 months	Cooperation Group starts its tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
9 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 - consistency of Member States' identification of OES
May 2021	57 months (i.e. 3 years after transposition)	Commission review



Thank you



PO Box 1309, 710 01 Heraklion, Greece



Tel: +30 28 14 40 9710



info@enisa.europa.eu



www.enisa.europa.eu

