



# Implementing The NIS Directive

Steve Purser | Head of Core Operations

8 June 2016 | NLO Meeting | Athens

European Union Agency for Network and Information Security



# Agenda



- 01** The ENISA Approach
- 02** The NIS Directive – Key Points
- 03** The Cooperation Group & The CSIRT Network
- 04** National NIS (Cybersecurity) Strategies
- 05** Incident Notification & Security Requirements
- 06** Standardization & Certification
- 07** Final Provisions
- 08** Role of the NLO



# The ENISA Approach



# ENISA Activities



## Recommendations



## Mobilising Communities



## Policy Implementation



## Hands on



CERT Exercises Handbook  
Document for teachers  
Deliverable – 2012-11-26

# The NIS Directive : Key Points





# The NIS Directive



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

**Status:** Possible adoption April 2016.

## **Key Provisions:**

- Obligations for all Member States to adopt a National NIS strategy and designate National Authorities.
- Obliges Member States to designate national competent authorities and CSIRTS.
- Creates first EU cooperation group on NIS, from all Member States.
- Creates an EU national CSIRTS network.
- Establishes security and notification requirements for operators of Essential Services (ESP) and Digital Service Providers (DSP).

# Structure



- Article 1 – Subject matter and scope
- Articles 2 & 3 – Minimum harmonization and definitions
- Article 5 – National NIS strategy
- Article 6 – National competent authorities and single point of contact
- Article 7 – Computer Security Incident Response Teams
- Article 8 – Cooperation Network
- Article 13 – International cooperation
- Article 14 – Security requirements and incident notification
- Article 15 – Implementation and enforcement
- Article 16 – Standardisation
- Article 17-20 – Penalties, Committee procedure, Review, Transitional measures
- Articles 21-23 – Transposition, Entry into force, Addressees

# The NIS Directive



National  
Cyber  
Security  
Strategies




Cloud Computing Services



Online Marketplaces



Search Engines


 **Strategic**  
Cooperation Network

**Digital Service Providers**

**Operators of Essential Services**

Incident Reporting

Security Requirements

 **Tactical/Operational**  
CSIRT Network

  
Transport

  
Energy and Water

  
Healthcare

  
Banking and Financial  
market infrastructures

  
Digital Infrastructure



# General role of ENISA



- Assistance to Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance to Member States in developing national NIS strategies.
- Participation within the EU NIS Cooperation Group.
- Provide secretariat support for the CSIRT network.
- Support the Commission in developing security and notification requirements for ESP and DSP.
- Assistance to Member States in developing national CSIRTs.
- Elaborate advices and guidelines regarding standardization in NIS security, together with Member States.



# The Cooperation Group & the CSIRT Network



# National competent authorities & single point of contact



- Member States have to designate *one or more* National Competent Authorities.
  - Monitor application of the Directive at national level.
- Member states also have to designate a Single Point of Contact
  - This is a liaison function to ensure cross-border cooperation of Member State authorities and between the **Cooperation Group** and the **CSIRTs network**.

# CSIRTs



- Member States have to designate *one or more* Computer Security Incident Response Teams (CSIRTs).
  - Responsible for handling incidents and risks according to a well-defined process.
  - A CSIRT may be established within a competent authority.
- Where they are separate, the competent authority, the single point of contact and the CSIRT will cooperate to fulfil the requirements of the Directive.

# The Cooperation Group



- The role of the group is (amongst other things) to:
  - Establish a work programme of actions
  - Provide strategic guidance for the activities of the CSIRT network
  - Discuss modalities for reporting notifications of incidents
  - Examine on an annual basis the incident summary reports
  - Periodically review of the functioning of the Directive
  - Discuss with representatives from the relevant European Standardisation Organisations, the standards referred to in the directive.
- As part of the group, ENISA will directly support with:
  - Exchange of best practices
  - Capacity building in NIS
  - Assistance in identification of ESPs

# The CSIRT Network



- Composed of MS CERTs and CERT EU.
- ENISA provides the secretariat and actively supports cooperation.
- The CSIRT network will:
  - Exchange information on CSIRT services, operations and cooperation.
  - Exchange and discuss information related to particular incidents at the request of an MS and/or on a voluntary basis.
  - Inform the Cooperation Group on its activities.
  - Discuss lessons learnt from Exercises
  - ....





# National NIS Strategies



# National NIS Strategies

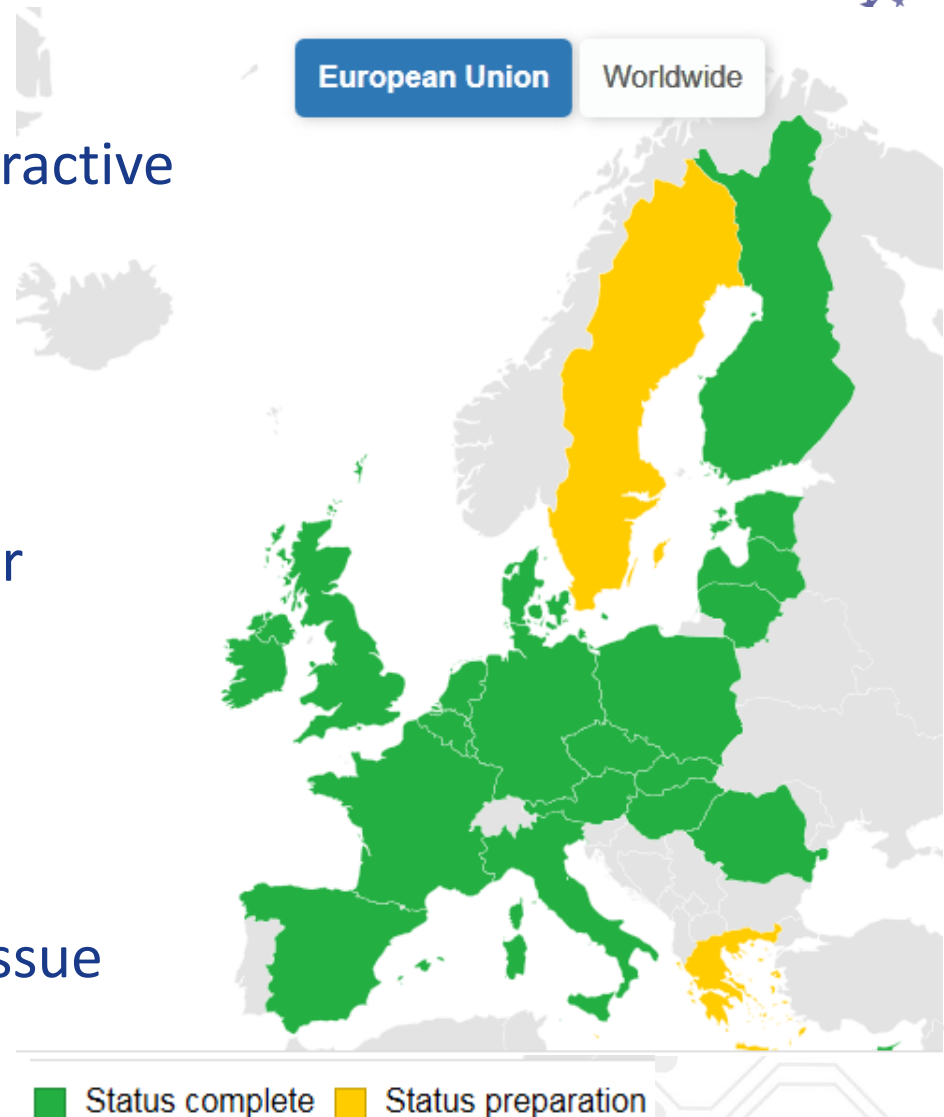


- Each Member State shall adopt a national NIS Strategy.
- The National NIS strategy covers:
  - Objectives & priorities
  - A governance framework.
  - Measures on preparedness, response & recovery.
  - Education & awareness programmes
  - Research & development plans
  - A risk assessment
  - List of involved actors.

# National Cyber Security Strategies (NCSS)

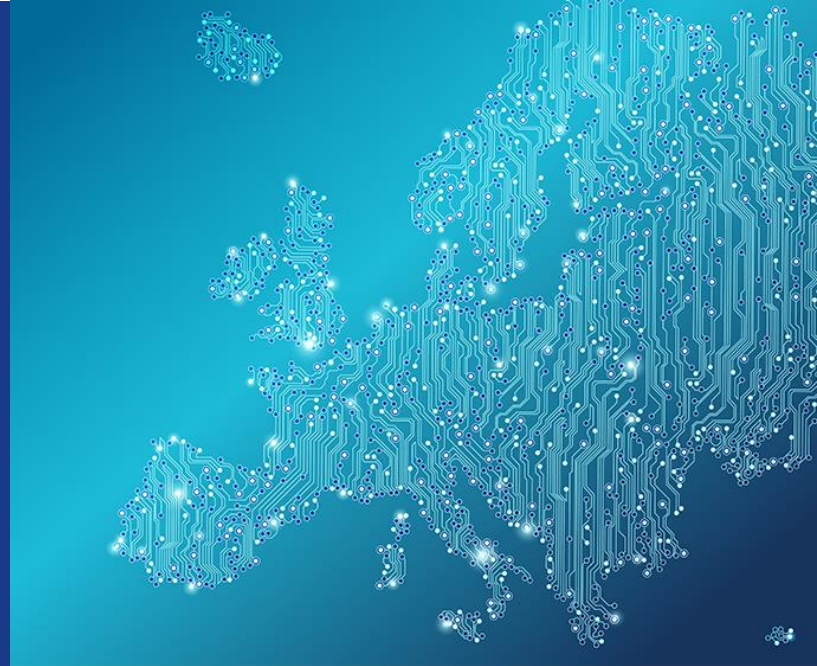


- A new version of NCSS interactive map on ENISA website
- Different maturity levels
- CIIP - key subject in NCSSs
- PPPs - limited success so far
- SMEs not properly covered
- Overlaps in authorities and mandates
- Assessment of NCSS is an issue





# Incident Notification & Security Requirements



# ENISA's role in developing security and notification requirements



- Incident reporting schemes and minimum security measures are required by the directive for:
  - ESP (energy, transport, financial, health, water, digital) and
  - DSP (search engines, cloud computing, online market places).
- Based on previous experience (mandatory incident reporting in telecom) ENISA is already providing support the Commission in developing the implementing acts for DSPs.
- Where ESPs are concerned, the initiative is with the Member States, but ENISA will provide support on an 'as needed' basis.

# Essential Service Providers (ESP)



- ESPs (energy, transport, financial, health, water, digital) should report to the designated authorities incidents related to the security of their services and take appropriate security measures according to the level of risk.
- Identification of ESPs devolves into the obligations of MS, ***but ENISA can assist within this process, as previous work has already been done in this area.***
- ***Future work is envisaged in this area, in ENISA WP2017 (Guidelines for identification of ESP, Guidelines for Incident reporting for ESP, Security measures for ESP).***



# Digital Service Providers (DSP)



- DSPs (search engines, cloud computing, online market places) are also imposed incident notification obligations and optional security measures.
- Within 1 year following the adoption of the NIS Directive, EC with ENISA, will develop two implementing acts to facilitate the uniform application of these obligations by MS across EU.
- Based on previous experiences ENISA will support the Commission with the following projects:
  - Guidelines for incident reporting within the NIS directive (DSP)
  - Security measures for DSPs in the context of NIS directive



# Standardization & Certification



# ENISA's role in standardization



- The NIS directive encourages the use of European or internationally accepted standards and/or specifications relevant to security of networks and information systems.
- ENISA, together with MS, shall elaborate advice and guidelines regarding standardization in NIS security.



# Final Provisions

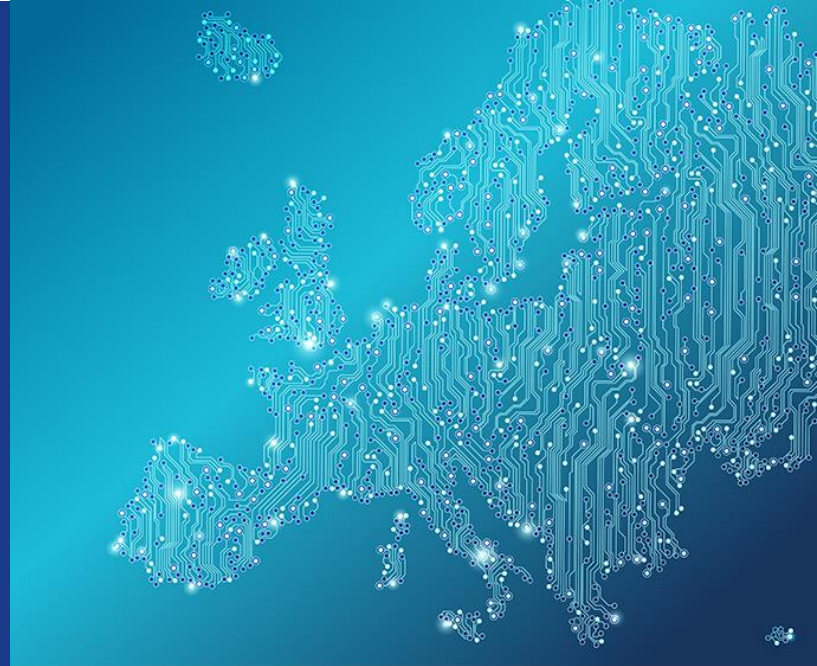


# Final Provisions



- Member States define the rules on penalties.
- The Commission will be supported by the Network & Information Security Committee.
- The Commission will submit a report to the Parliament and the Council one year after the date of transposition.
- The transposition period is 21 months.

# Role of the NLO





# The Role of the NLO



- The NLO network is one of the principle mechanisms ENISA uses to exchange information with the Member States.
- A lot of the NIS Directive is concerned with communication – the challenge is to bridge this communication with the communication carried out in the NLO network.
- Industry remains an important challenge for ENISA. Engaging new industry sectors is very difficult.
- We also need to align with the Commission’s cPPP that will be launched this year.
- This will be discussed at the end of today.



# Thank you

 PO Box 1309, 710 01 Heraklion, Greece

 Tel: +30 28 14 40 9710

 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

