NIS Directive

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

• **Status:** ADOPTED July 2016.

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

• **Provisions:**
  • Improved cybersecurity capabilities at national level
  • Increased EU-level cooperation
  • Obligations for operators of essential services (OES)
  • Obligations for digital service providers (DSP)
# NISD Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>entry into force + ...</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2016</td>
<td>-</td>
<td>Entry into force</td>
</tr>
<tr>
<td>February 2017</td>
<td>6 months</td>
<td>Cooperation Group begins tasks</td>
</tr>
<tr>
<td>August 2017</td>
<td>12 months</td>
<td>Adoption of implementing on security and notification requirements for DSPs</td>
</tr>
<tr>
<td>February 2018</td>
<td>18 months</td>
<td>Cooperation Group establishes work programme</td>
</tr>
<tr>
<td>May 2018</td>
<td>21 months</td>
<td>Transposition into national law</td>
</tr>
<tr>
<td>November 2018</td>
<td>27 months</td>
<td>Member States to identify operators of essential services</td>
</tr>
<tr>
<td>May 2019</td>
<td>33 months (i.e. 1 year after transposition)</td>
<td>Commission report assessing the consistency of Member States' identification of operators of essential services</td>
</tr>
<tr>
<td>May 2021</td>
<td>57 months (i.e. 3 years after transposition)</td>
<td>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</td>
</tr>
</tbody>
</table>
NIS Directive
DSPs & OESs Obligations

Commonalities
- Security measures
- Incident notification

Differences
- Identification criteria
- Audit
- Implementing Acts
- Light touch approach
- Medium & Large enterprises
DSPs obligations

- Substantial impact of an incident
- Security measures:
  - security of systems and facilities
  - incident handling
  - business continuity management
  - monitoring, auditing and testing
  - compliance with international standards
OES obligations

EC Cooperation Group

Identification Criteria DE
Security Measures FR
Incident reporting NL
Cross-border Interdependencies EE

Identification Criteria for OES
Security Measures for OES
Incident Reporting for OES
Cross border Interdependencies

ENISA
# OES Identification criteria – MS 2016 Overview

<table>
<thead>
<tr>
<th></th>
<th>CZECH REPUBLIC</th>
<th>ESTONIA</th>
<th>GERMANY</th>
<th>LATVA</th>
<th>LITHuania</th>
<th>MALTA</th>
<th>POLAND</th>
<th>SWITZERLAND</th>
<th>NETHERLANDS</th>
<th>HUNGARY</th>
<th>ROMANIA</th>
<th>FRANCE</th>
<th>THE SLOVAK REPUBLIC**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Individual customers</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Impact on the MS economy</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public confidence/trust</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>International relations</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inter - sector dependencies</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Cross - sector dependencies</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Public order and public safety</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Impact on societal activities</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>3rd party MS services are affected</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

** Information based on current state on internal discussions between national authorities
Security Measures for OES

GOVERNANCE AND ECOSYSTEM
- Information system security governance & risk management
- Ecosystem management

PROTECTION
- Identity and access management
- IT Security Administration
- IT Security Architecture
- IT security maintenance
- Physical and environmental security

RESILIENCE
- Detection
- Computer security incident management

DEFENSE
- Continuity of Operations
- Crisis Management
Incident Reporting for OES: the process
Cross border interdependencies: Proof of concept
CSIRTs Network

- SOPex
- CSIRTs Network Meeting: Sophia, end of March
Challenges vs Key success factors

• Low engagement of MSs

• Diverse views regarding the approaches & thresholds definitions

• Different security requirements stemming from other regulations e.g GDPR

• Active support with facilitation, surveys and stock takings and reports

• Engage private sector to harmonize and gain knowledge

• Build trust amongst the members of the CG and the CSIRTs network
## ENISA’s role in the NISD

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Assist MS and the EU Commission</td>
</tr>
<tr>
<td>02</td>
<td>Participate in the EU NIS Cooperation Group</td>
</tr>
<tr>
<td>03</td>
<td>Secretariat for CSIRTs Network</td>
</tr>
<tr>
<td>04</td>
<td>Elaborate advices and guidelines regarding standardization in NIS security</td>
</tr>
<tr>
<td>05</td>
<td>Organize exercises</td>
</tr>
</tbody>
</table>
ENISA’s activities 2018

Contributing to the Cooperation Group
Supporting policy discussions, engagement and dialogue with stakeholders
Establishing working relations with industry working groups

Stocktaking and recommendations on security measures, incident reporting audit frameworks

More technical reports:
• Mapping of OES Security Requirements to Specific Sectors (Energy, Transport, etc ...)
• Dependencies of OES on DSPs in Healthcare, Finance & Aviation sectors.
• ...