The Cybersecurity Package and the new role of ENISA

CA Day, 24th October 2018
Sławomir Górniak
Positioning ENISA activities

**CAPACITY**
- Hands on activities

**POLICY**
- Support MS & COM in policy implementation
- Harmonisation across EU

**COMMUNITY**
Mobilizing EU communities

**EXPERTISE**
- Recommendations
- Independent Advice
“Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks.

[...] 

Today, the Commission is proposing new tools, including a European Cybersecurity Agency to help defend us.”
Cybersecurity Package

- **Commission Proposal for a Cybersecurity Act**: Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") – COM(2017) 477


- **Blueprint**: Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises – (C(2017) 6100)

- **Commission Communication “Making the Most of NIS”**: towards effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (COM(2017) 476)
# The Proposed “Cybersecurity Act”

## Six key objectives:

1. Increasing **capabilities** and **preparedness** at EU and MS level

2. Improving **cooperation** and **coordination** of stakeholders

3. Increasing EU level capabilities to **complement** MS action

4. Promoting cybersecurity **awareness** in the EU

5. Increasing **transparency** of cybersecurity assurance

6. Avoiding **fragmentation** of certification schemes
The proposed “Cybersecurity Act”

The proposal contains important new/revised tasks for ENISA:

- **Strengthened and reinforced ENISA; substantially altered:**
  - Role in policy development and implementation
  - Role in operational cooperation – Blueprint
  - Participation in research funding programmes

- **EU-level cybersecurity certification framework with:**
  - A role for ENISA in the preparation of candidate schemes
  - Secretariat assistance provided by ENISA for the “European Cybersecurity Certification Group”
Why ENISA Reform?

- Need for enhanced role for ENISA with:
  - Adequate Resources
  - Permanent Status
  - A Stronger Mandate

Reformed ENISA (EU Cybersecurity Agency)
Proposed Tasks for a Stronger ENISA with a **Permanent** Mandate:

<table>
<thead>
<tr>
<th>Law and Policy Tasks</th>
<th>Capacity Building</th>
<th>Operational Cooperation</th>
<th>Market and Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Awareness Raising</strong></td>
<td><strong>Research and Innovation</strong></td>
<td><strong>International Cooperation</strong></td>
<td></td>
</tr>
</tbody>
</table>
EU Cybersecurity Certification Framework Proposal – Background

Defining certification:

“the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated” (*)

“formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance” (**)

- Security certification of products has been traditionally dominated by Common Criteria
- Within EU
  - SOG-IS MRA is the dominant player in common criteria certification
  - Multiple national and sectorial initiatives focused on security certification
ICT security certification in the EU

- Network and Information Security Directive
- eIDAS Regulation
- Payment Services Directive 2
- General Data Protection Regulation
- Proposal for a Regulation on Privacy and Electronic Communications

Digital Single Market Strategy

- Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
Possible features of an EU certification framework

- Avoid fragmentation caused by national ICT security certification initiatives
- Promote mutual recognition
- Defined assurance levels (Basic, Substantial, High)
- Simplify procedures, reduce the time and cost of deployment of IT products and services
- Improve competitiveness and quality of European products and services
- Give users more confidence in ICT products and services they purchase
The Cybersecurity Package and the new role of ENISA

Putting certification schemes forward
Putting certification process forward
Key elements of the proposed framework

<table>
<thead>
<tr>
<th>Scheme scope including: type and categories of processes, products and services covered</th>
<th>Reference to standards followed in the evaluation process</th>
<th>Specific cybersecurity requirements for CABs as appropriate</th>
<th>Specific evaluation criteria and methods used</th>
<th>Information to be supplied to CABs by applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions to use marks and labels</td>
<td>Rules for monitoring compliance of the certificates or the EU declaration of conformity</td>
<td>Rules to report vulnerabilities</td>
<td>Rules to report vulnerabilities</td>
<td>Rules to report vulnerabilities</td>
</tr>
<tr>
<td>Conditions to grant maintain and extend a certificate</td>
<td>Records keeping in CABs</td>
<td>Records keeping in CABs</td>
<td>Records keeping in CABs</td>
<td>Records keeping in CABs</td>
</tr>
<tr>
<td></td>
<td>Identification of national/intl schemes in the same area</td>
<td>Identification of national/intl schemes in the same area</td>
<td>Identification of national/intl schemes in the same area</td>
<td>Identification of national/intl schemes in the same area</td>
</tr>
<tr>
<td></td>
<td>Content of issued certificate or EU declaration of conformity</td>
<td>Content of issued certificate or EU declaration of conformity</td>
<td>Content of issued certificate or EU declaration of conformity</td>
<td>Content of issued certificate or EU declaration of conformity</td>
</tr>
<tr>
<td></td>
<td>Period of validity</td>
<td>Period of validity</td>
<td>Period of validity</td>
<td>Period of validity</td>
</tr>
<tr>
<td></td>
<td>Disclosure policy</td>
<td>Disclosure policy</td>
<td>Disclosure policy</td>
<td>Disclosure policy</td>
</tr>
<tr>
<td></td>
<td>Mutual recognition</td>
<td>Mutual recognition</td>
<td>Mutual recognition</td>
<td>Mutual recognition</td>
</tr>
</tbody>
</table>
Drawing up the promulgation of a certification scheme

- **Open**: a scheme to be drawn up by means of open consultations accessible to all parties interested in the technology, products or services affected by the said scheme.

- **Consensus seeking**: The consultation process to be collaborative and consensus based refraining from favouring any particular stakeholder.

- **Transparent**: Any new scheme activity to be publicised broadly through means available to ENISA. Information concerning technical discussions and consultations to be recorded. Feedback received during the consultation process to be treated in an equitable manner and responses to be provided for.
Current ENISA certification activities

- Supporting policy discussions, engagement and dialogue with stakeholders
- Establishing working relations with industry working groups
- Stocktaking on the development of a European ICT security certification and labelling framework
- Analysing the ICT security certification laboratories landscape in the EU
- Seeking to engage towards the EU framework based on existing schemes and responding to emerging lightweight requirements
Messages to take away

• The Cybersecurity Package is an important step in assuring resilience of European networks

• ENISA with a new mandate will stronger support European cybersecurity

• The new ICT security certification framework will improve competitiveness and quality of European ICT products and provide for more confidence

• ENISA will actively contribute to the certification framework
Thank you

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu