NIS Platform

Trust and Security Unit
DG Communications Networks, Content and Technology

Ann-Sofie Rönnlund
Policy Officer

24.11.2014
Preliminary Workshop comparing U.S. Cybersecurity framework and EU NIS Platform approaches

EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace

Digital Agenda for Europe

1. Cyber resilience
   - NIS Directive (capabilities, cooperation, risk management, incident reporting)
   - Raising awareness

Justice and Home Affairs

2. Reduce cybercrime

EU Foreign and Security Policy

3. Cyber defence policy and capabilities
5. International cyberspace policy

4. Industrial and technological resources: NIS platform; H2020

- Fundamental rights apply both in physical and digital world
- Cybersecurity depends on and contributes to protecting fundamental rights
- Access for all
- Democratic and efficient multi-stakeholder governance
- Cybersecurity is a shared responsibility

NIS Platform

State of play and achievements

The NIS Public-Private Platform

- **A key action of the EU Cybersecurity Strategy**
  - **Identify and develop incentives to adopt good cybersecurity practices**
  - **Promote the development and the adoption of secure ICT solutions**

  - **Draw from working practices, incl. relevant standards**
  - **Process-related and technoly-neutral**
  - **Incentives for voluntary adoption**
  - **Cross-cutting / horizontal approach**
  - **Focus on SMEs**

Working Groups and deliverables

- **WG1: risk management**
  - **Guidance document (04/2014)**
- **WG2: information sharing and incident notification**
  - **Guidance document (04/2014)**
- **WG3 on secure ICT research and innovation**
  - **Stakeholder views for H2020 WP 2016 and beyond**
  - **Business cases and innovation (Q4 2014)**
  - **Education and training (Q2 2015)**

Participants

- **An inclusive and multi-stakeholder platform**
  - **Driven by the participants**
  - **More than 200 participants**
  - **18 MS + Norway: ministries, NIS agencies, NRAs, CERTs**
  - **Research & academia**
  - **Industry: ICT, finance, post, transport, healthcare, defence, energy, water sectors**

Resources

- **Commission and ENISA provide operational support to the chairs; rapporteurs in the future**
- **Online portal**
  - **Working & publication tool**
  - **https://resilience.enisa.europa.eu/nis-platform**

NIS Platform

Next steps

Proposed next steps

- **Input into Commission recommendations on good cybersecurity practices (2015)**
  - **Organisational structures and requirements**
  - **Verification and auditing of requirements**
  - **Voluntary information sharing**
  - **Incident response**
  - **Mandatory incident notification**
  - **Code of conduct on data protection**
  - **[Incentives]**
- **Provide input to the secure ICT R&I agenda at EU, national and industry level**
- **Contribute to consistent implementation of the NIS Directive**

Possible future topics

- **"In the future the need may arise for NIS Platform to give views on new standardisation needs, as input to work ongoing in other for a (e.g. ETSI, CSCG, the Multi-Stakeholder Platform for ICT Standardisation or other) on the potential need for sector-specific recommendations (cf. work led by ENISA on smart grids), or for the development of cyber-insurance."**

Related activities

- **"The NIS Platform will be asked to work closely together with related groups in the standardisation and certification fields, such as ETSI, CSCG and MSP.**

- **The NIS Platform will also be asked to compare its results with work and experiences of international partners, studying for example the work initiated by NIST in the USA."**

Thank you for your attention

Questions?

CNECT-NIS@ec.europa.eu

NIS Platform Documents:

- *https://resilience.enisa.europa.eu/nis-platform*