ICT/MSP (2013) 044
21/1/2012

European Multi-Stakeholder Platform on ICT Standardization

Meeting: **7 February 2012**

Title document: **Cyber Security Strategy of the EU**

Submitter: EU

Document for:

Information	✔
Decision	
Discussion	

Email:ec-ict-std-platform@ec.europa.eu

Cyber Security Strategy of the EU - Standardisation Multi Stakeholder Platform meeting, 7 February 2013.

WHAT ARE THE TOOLS?

- Joint Communication on the "Cyber Security Strategy of the European Union".
- Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union.
- The Joint Communication and Proposal for a Directive are expected to be launched in Q1 2013.

WHAT IS THE ISSUE?

- Digital technologies and the Internet are the backbone of our society and economy and are key enablers of prosperity and freedom. A high level of cybersecurity across the EU is essential to preserve the well-functioning of the internal market as well as growth and jobs.
- The magnitude and frequency of deliberate or accidental incidents on networks and information systems is increasing and can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the EU.
- The current situation in the EU does not provide sufficient protection against these incidents. The existing capabilities and mechanisms are insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all Member States.

WHY DOES ACTION HAVE TO BE TAKEN BY THE EU?

- As network and information systems are globally interconnected, cybersecurity does not stop at borders. We need to have no weak links across the EU.
- Lack of intervention at EU level would lead to a situation where each Member State would act alone disregarding the interdependences amongst network and information systems. Action at EU level would ensure that an appropriate degree of coordination takes place among the Member States so that governments' measures are consistent with each other, and risks are well managed in the cross-border context in which they arise.

WHAT ARE THE GOALS?

- A high level of cybersecurity across the EU in terms of increased capabilities, preparedness, cooperation, information exchange and awareness at national and EU level, both in the public and the private sectors.
- Considerable improvement in the protection of EU consumers, business and Governments against networks' incidents, threats and risks.
- Member States' ensure preparedness both in terms of technical and organisational capabilities.

- Coherent and coordinated prevention and response to cross-border incidents and risks through the set-up of a mechanism for cooperation at EU level.
- The introduction of requirements to carry out NIS[1] risk management for public administrations and key private players. The obligation to report incidents with a significant impact will enhance the ability to respond to incidents and foster transparency.

WHERE DO STANDARDS COME IN?

- We foresee actions on the promotion of the development and of the take-up of ICT security standards. However, not having as yet identified gaps in the currently available security standards, no mandates are planned at this point.
- The focus will be on establishing a number of reference standards and/or specifications relevant to network and information security, including, where relevant, harmonized standards, to serve as a basis for encouraging the coherent adoption of standardisation practises across the Union.
- The type of standardisation initially aimed at is "soft guidance" built, using a combination of existing standards, best practice and minimum security requirements. Areas of interest may include:
    - minimum cybersecurity performance requirements to be applied to ICT products used in Europe and certification schemes
    - technical guidelines and recommendations for the adoption of NIS standards and good practices
    - security-by-design industry-led standards, technical norms and principles for ICT product manufacturers and service providers
    - industry-led standards to assess companies' performance on cybersecurity and security labels
    - standards related to information exchange environments (threat intelligence, vulnerabilities, etc)

WHAT IS THE ENVISAGED ROLE FOR THE MSP?

- A constructive dialogue and input related to the Commission's standardisation activities (identifying gaps, establishing reference standards) in Network and Information Security.
- Actively assist the Commission and ENISA to develop technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

[1] Network and Information Security