Towards a EU policy on critical information infrastructure protection (CIIP)

Andrea Servida
European Commission
DG INFSO-A3
Andrea.servidaa@ec.europa.eu
NIS: a cross-cutting issue @ EC

**DG INFSO**
- NIS policy
- CIIP
- e-Signature & eID
- e-privacy
- SPAM
- harmful content
- FP7 ICT theme
- IPv6

**DG JLS**
- Cyber crime
- EPCIP & support programme
- Data protection
- Data retention
- Travel documents
- Identity theft

**DG MARKT**
- e-payment
- e-frauds
- ...

**DG ENTR**
- SME’s & NIS
- standards
- FP7 Security theme

**DG JRC**
- Support to policy DG
- Specific R&D
- ...

**DGIT/ADMIN-DS**
- e-Commission
- IDABC
- Internal security rules…
NIS Policy and related Regulations (1)

  - holistic approach for a comprehensive EU-wide strategy across “pillars”, related policy and regulatory initiatives
  - “voluntary” activities stakeholders via dialogue, partnership and empowerment
  - reinforce ENISA’s role in implementing the EC policy
  - importance of “resilience” strategy for CIIP, i.e. the ability to deal with unexpected events

- **Other initiatives related to NIS**
  - fighting against spam, spyware and malware [COM(2006)688]
  - promoting data protection by PET [COM(2007)228]
  - fighting against cyber crime [COM(2007)267]
• **NIS in the eCommunications Review**
  - Security and integrity (Art 13 FW D)
    - level of security appropriate to risks
    - prevent/minimise impact of security incidents on users and interconnected networks
    - focus on continuity of supply of services
  - Responsibilities of operators
    - stronger obligations to ensure security and integrity (Art 13 FW D)
    - mandatory breach notifications
      - to NRA (Art 13 FWD): significant impact on operations
      - to consumers and NRA (Art 4 e-privacy D): personal data compromised
  - Technical measures (Art 13 FW D)
    - The Commission (“... *taking the utmost account of the opinion ...*) may adopt appropriate technical implementing measures with a view to harmonising
European Network and Information Security Agency (ENISA)
- Established in March 2004 with a 5 yrs mandate
- Extension of the mandate for 3 yrs formally adopted in September

What’s ahead?
- A public debate on objectives and means for a reinforced NIS policy in the EU
- A policy initiative on Critical Information Infrastructure Protection (CIIP)
Public debate on NIS policy

- Broader thinking on NIS is essential
- Commissioner Reding called on EP and Council to open an intense debate on Europe’s approach to network security and on how to deal with cyber-attacks
- Calls were made both in EP and Council for a debate on further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security
- Aim and Scope:
  - Possible objectives for a modernised and reinforced NIS policy at EU level, and the means to achieve those objectives
Public Consultation “Towards a Strengthened NIS Policy in Europe”

- The Commission launched an on-line public consultation (07/11/08 – 09/12/09)
  - challenges to NIS
  - priorities of a modernised NIS policy
  - means needed to address the challenges

- The European Council will be involved
  - Telecom Working Group March
  - Planned Ministerial Conference (tentatively on 27-28 April 2009)
  - Exchange of views at the European TTE Council on 12 June 2009 – Presidency guidelines
Policy initiative on CIIP – Q1 2009: The issues at stake / Rationale

- CII are the nervous system of the Information Society
- Liberalisation, deregulation and convergence → complexity / multiplicity of players
- Infrastructures are privately owned and operated
- Ensuring the stability of society and economy is governments’ responsibility
- CII stretch out well beyond national borders
- The level of security in any country depends on the level of security put in place outside the national borders
- National governments face very similar issues and challenges
- The private sector is calling for harmonised rules

→ A more integrated and co-ordinated approach to complement and add value to the national programmes
→ Contribute to reinforce the EU wealth creation capabilities
Planned policy on CIIP

• Goal
  - Protect Europe from large scale cyber attacks and disruptions
  - Promote security and resilience culture (first line of defense) & strategy
  - Tackle cyber attacks & disruptions from an ecosystem perspective

• Aims
  - Enhance the CIIP preparedness and response capability in EU
  - Promote the adoption of adequate and consistent levels of preventive, detection, emergency and recovery measures
  - Foster International cooperation, in particular on Internet stability and resilience

• Approach
  - Build on national and private sector initiatives
  - Engage public and private sectors
  - Adopt all-hazards
  - Be multilateral, open and all inclusive
Planned policy initiative on CIIP

**Priority areas (1)**

- **Preparedness and prevention**
  - European Public Private Partnership on Resilience
  - Baseline of capabilities and services for National/Gov CERTs for pan-European cooperation
  - European Forum for Member States to exchange good policy practices

- **Detection and response**
  - Prototyping a European Information sharing and alert system
Planned policy initiative on CIIP

Priority areas (2)

- Mitigation and recovery
  - Cooperation between European National/Gov CERTs
  - Promote national contingency planning for incident response and disaster recovery
  - Promote pan European exercises on simulated large-scale public network security incidents
Planned policy initiative on CIIP

priority areas (3)

• International Cooperation

– Internet long term resilience and stability
  • EU priorities on security and resilience of critical components (i.e. DHCP, DNS, MPLS)
  • Principles and guidelines for Internet resilience and stability (focus on remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data)

– Global co-operation on exercises on large-scale network security incidents exercise
Planned policy initiative on CIIP
priority areas (4)

• ICT sector specific criteria
  – continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria
  – A study is being launched
  – Staff Working Paper on criteria
TIMELINE OF THE CIIP INITIATIVE: implementation activities

- **2008**
  - Formal adoption of the EPCIP Directive (4Q 08)
  - Stock taking of the implementation (1Q 10)
- **2009**
  - Adoption of Communication on CIIP (March 09)
  - Proposal to strengthen the NIS policy at the EU level after the end of the ENISA mandate (1Q 10)
- **2010**
  - Public consultation on a modernised NIS policy (Nov 08-Jan 09)
- **2011**
  - Debate on a modernised NIS policy (Jun 08-Dec 09)
- **2012**
  - End of the ENISA mandate

**Notation**
- Study
- EC document
- Public consultation
- On-going consultation
- Meeting
- New project
- Planned activity
Policy initiative on CIIP: Next steps – short term

- **End of January 2009**
  - Procedure for formal adoption of Communication + Impact Assessment

- **5 February 2009**
  - Workshop with MS on DNSSEC deployment

- **March 2009**
  - Adoption of Commission policy on CIIP

- **31 March 2009**
  - Workshop on vulnerability disclosure

- **27-28 April 2009**
  - *Ministerial Conference on CIIP and the future of NIS in the EU*
Policy initiative on CIIP: Next steps - Medium term (1/2)

- **Studies and projects soon starting**
  - A study on dependencies on ICTs of finance, energy and transport sectors*
  - Grants for prototyping a European multilingual information sharing and alert system to provide appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices*
  - Grant for a project on DNS resilience*

- **Studies being launched**
  - A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet*
  - A study to support the process to define sectoral criteria to identify European Critical Infrastructures in the ICT sector focusing on the sub-sectors of Internet, fixed and mobile telecommunications*

*Projects and studies funded under EPCIP financial scheme: "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"
Policy initiative on CIIP: Next steps - Medium term (2/2)

• Call for Tenders & for Proposals in 2009

- Grant for the development, implementation and evaluation of a large-scale pan-European exercise to test Internet contingency plans*
- Grant for the development of national business case for the implementation of priority communications capability on public networks*
- Study on public-private partnership initiatives to enhance security and resilience of fixed and mobile telecommunications as well as the Internet*
- Grant for the development of inter-dependency modelling tools for the ICT sector*
- Study aiming the development of a methodology and research of quantitative data on the economics of security and resilience in CII (tentative)
- Study on the security and resilience challenges brought about the convergence towards IP networks (tentative)

* Projects funded under EPCIP financial scheme: "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"
Web Sites

EU policy on secure Information Society

Page on CIIP activities

Page on ARECI study

Page on the workshop on large scale attacks

Public consultation “Towards a Strengthened Network and Information Security Policy in Europe”
http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4464
http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=InfsoNis
Links to EU Policy Document (1/2)

  http://eur-lex.europa.eu/Result.do?T1=V5&T2=2006&T3=251&RechType=RECH_natural&Submit=Search

- **Fighting spam, spyware and malicious software [COM(2006)688]**
  http://eur-lex.europa.eu/Result.do?T1=V5&T2=2006&T3=688&RechType=RECH_natural&Submit=Search

- **Promoting data protection by Privacy Enhancing Technologies (PETs) [COM(2007)228]**
  http://eur-lex.europa.eu/Result.do?T1=V5&T2=2007&T3=228&RechType=RECH_natural&Submit=Search

- **Towards a general policy on the fight against cyber crime [COM(2007)267]**

• European Programme for Critical Infrastructure Protection [COM(2006) 786]

• Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection
  
  Press release:
  Final text:

• EPCIP financial scheme: "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"
  
  Call for proposals
  http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

  Call for tenders
  http://ec.europa.eu/justice_home/funding/tenders/funding_calls_en.htm

  Call for expression of interest (looking for external experts)
  http://ec.europa.eu/justice_home/funding/tenders/funding_interest_en.htm