

# ***A Strategy for a secure Information Society – “Dialogue, Partnership and empowerment”***

**Gerard.Galler@ec.europa.eu**  
**European Commission**

DG Information Society & Media

Unit INFSO/A3: Internet; Network & Information Security



# Why a new strategy?

- Base:
  - Communication of European Commission (31.5.06),  
Resolution of EU Council (11.12.06)
- Objective: to revitalise EC's strategy of 2001
  - New business and technical **paradigms**
  - Security became a **political** issue
  - Increasing focus on the protection of **critical infrastructures**
  - To improve coordination between the various EC policy initiatives
  - To answer the demand of EU and international stakeholders to cooperate
  - To take the "new born" **ENISA** into account
  - To stimulate a **risk management** approach



# The Challenges (1/2)

- **Technical Dimension**
  - Threat landscape changes (criminality)
  - Convergence of digital services
  - Pervasiveness of ICT
  - Mobile computing, wireless connectivity
- **Economic dimension**
  - Make the EU ICT industry a competitive supplier
  - Private and public sectors as demanding users
    - Security seen as an advantage instead of a cost
  - Economical dependence on ICT security
  - Financial loss due to poor risk preparedness



# The Challenges (2/2)

- **Social dimension**

- Citizens & consumers may become “vehicles” of attacks
- Societal dependence on ICT
- Protection of fundamental rights. Balance between NIS policies and civil liberties

- **Legal dimension**

- A substantial body of legislation relevant to NIS exists
  - Need for new legal and/or regulatory measures. Need for coherence.
- Related EC texts:
  - Spam & malware,
  - Cybercrime, PET, Review of the telecom regulatory framework (may be: liability, leakages, safeguards, ...), Protection of critical information infrastructures



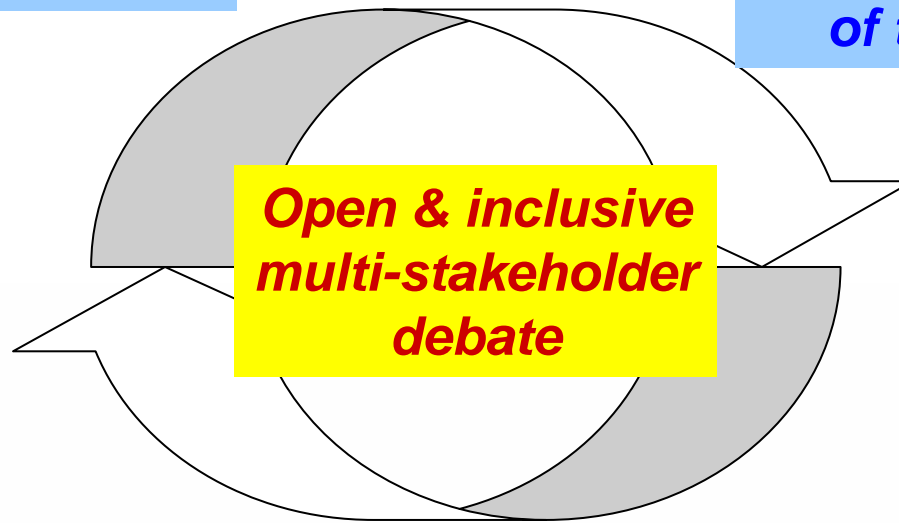
# Towards a secure Information Society

## **DIALOGUE**

*structured and  
multi-stakeholder*

## **PARTNERSHIP**

*greater awareness &  
better understanding  
of the challenges*



## **EMPOWERMENT**

*commitment to responsibilities  
of all actors involved*



# Dialogue

- **Exchange** of NIS-related policies between Member States
- Raise **awareness** and strengthen **trust** of SMEs + citizens on risks & solutions
- Agreement on a **Balance** between security and privacy protection
- Policy for **protection of critical infrastructures**
- **Industry commitment** to adopt a culture of security



# Partnerships

- **Improve knowledge of the problem**
  - Devise a data collection framework to collect EU-wide data on security incidents and consumer confidence
  - To gather data on trends in ICT security
- **Support response capability**
  - To **examine the feasibility** of a European information sharing and alert system (including a multi-lingual security portal)



# Empowerment

- **Invite EU Member States to:**
  - Promote **awareness** on benefits of security practices;
  - Transfer best practice of national NIS policies; Leverage e-Gov services to promote good practices;
  - Stimulate security in **higher education** curricula.
- **Invite private sector to take initiatives to:**
  - Develop definition of **responsibilities** for producers & ISP.
  - Work towards affordable security **certification** schemes for products, processes and services (including privacy).
  - Promote **diversity, openness, interoperability, usability** and **competition**.
  - Promote **training** programmes to provide employees with skills to implement security practices.
  - Developing **risk management** methods & culture of risk management in organisations



# Research: FP7–ICT: Secure, dependable & trusted infrastructures

- **Call 1** (opening 22.12.06, **closing 8.5.07**), Budget: 90 M€
  - Security and resilience in network **infrastructures**
    - Scalable, context-aware, secure & resilient architectures & technologies
    - Real-time detection and recovery against intrusions and failures
  - Security & trust in dynamic & reconfigurable **service** architectures
  - **Trusted computing** infrastructures
  - Security & dependability in the **engineering** of SW and service
  - **Identity** Management and **Privacy** enhancing tools
  - Coordination & Support Activities
- **Call 2 (2H2007):**
  - New paradigms and experimental facilities
  - Protection of **critical infrastructures** (joint call with FP7-Security)
- Information Day: 26.2.07, Brussels
- See <http://cordis.europa.eu/ist/trust-security/index.htm>



## COM(2006) 251 A Strategy for a secure Information Society – “*Dialogue, Partnership and empowerment*”

[http://ec.europa.eu/governance/impact/docs/ia\\_2006/com\\_2006\\_0251\\_en.pdf](http://ec.europa.eu/governance/impact/docs/ia_2006/com_2006_0251_en.pdf)

## SEC(2006) 656 Commission Staff Working Document – Impact Assessment

[http://ec.europa.eu/governance/impact/docs/ia\\_2006/sec\\_2006\\_0656\\_en.pdf](http://ec.europa.eu/governance/impact/docs/ia_2006/sec_2006_0656_en.pdf)

