WORKSHOP ON SECURITY CERTIFICATION FOR SMART GRIDS

27th June 2012

Alejandro PINTO
European Commission

Information Society and Media
Network and Information Security

alejandro.pinto-gonzalez@ec.europa.eu

EU Policy & Cooperation initiatives

- Policy context: NIS/CIIP
- Expert Group on Security and Resilience of communication networks and information systems for the Smart Grid
- European Cyber Security Strategy

CIIP ACTION PLAN

Five specific objectives:

1. Foster cooperation and exchange of good policy practices between Member States (EFMS)
2. Develop a public-private partnership at the European level on security and resilience of CIIs (EP3R)
3. Enhance incident response capability in the EU, promoting national and European cyber contingency plans and exercises on simulated large-scale network security incidents.
4. Reinforce international cooperation on global issues, in particular on resilience and stability of Internet

Communication on CIIP - COM(2009)149 - COM(2011)163

EU EXPERT GROUP ON SECURITY AND RESILIENCE OF COMMUNICATIONS NETWORKS AND INFORMATION SYSTEMS FOR SMART GRIDS

In 2010, the European Commission (EC), with the support of the European Network and Information Security Agency (ENISA), convened an Expert Group for:

- Identification and discussion about the related policy at EU level.
- Better understand of the views and objectives of the private and public sectors on the ICT security and resilience challenges for the smart grids by bringing Electricity and ICT communities together to discuss and work on relevant issues. The EG is compound by:
  - Member State authorities in charge of NIS , CIIP and energy;
  - ICT industry and industrial associations;
  - Organisations with experience in cyber security standards;
  - Electricity generators and industrial associations;
  - Distribution and transmission network operators and industrial associations;
  - Suppliers of automation and control systems and associated technologies;
  - Energy (and related, including emissions) trading entities;

Expert Group- Program of Work

2.1. Risks, threats and vulnerabilities

WP 1.1. Identify and categorize all relevant Smart Grid assets

WP 1.2. Develop an attack / threat taxonomy for relevant assets

WP 1.3. Develop a countermeasure taxonomy for relevant assets

WP 1.4. Develop a high-level security risk assessment methodology for relevant assets

2.2. Requirements and technology

WP 2.1. Security Requirements

WP 2.2. Extend Smart Grid requirements to include effective security measures

WP 2.3. Research Smart Grid communication protocols and infrastructures to incorporate data security measures

WP 2.4. (Public) procurement

2.3. Information and knowledge sharing

WP 3.1. Develop a cross-border alliance between Member States and relevant competent bodies and

2.4. Awareness, Education & Training

WP 4.1. High level Conference for strategic leaders

WP 4.2. Propose initiatives to increase stakeholder awareness on data security

WP 4.3. Skilled personnel on cyber security in energy industry

Timeline: From Nov 2010 to May 2012

Conclusions and Recommendations of the Expert Group

- **Education (skilled personnel on cyber security in energy industry):**
  - Lack of well-trained proactive decision-taking operators to operate the next generation Smart Grid infrastructure.
  - To meet this challenge might require updating engineering and ICT education curricula.

- **Risk Assessment**:
  - ICT and electricity security experts should work together to enhance the design of security in smart grids.
  - It is needed to carry out an overall risk assessment to identify the specific well-balanced and effective set of security measures to be adopted by relevant operators. Such evolving scenario requires regular reassessment.

Conclusions and Recommendations of the Expert Group

- **Risk Management:**
  - Define high level security requirements to enhance the security and resilience of ICT for Smart Grids.
  - Accomplishing security requirements based on security properties (confidentiality, integrity and availability) and along the dimensions of detection, response and recovery.

- **Incident management:**
  - Mandate to a governmental authority in charge of responding to incidents and managing crisis due to cyber-attacks on smart grid.

- **(Public) Procurement:**
  - Establishing a common procurement language and/or standard for a base level of security in smart grid components and services in collaboration with private and public asset owners, vendors and regulators.

Conclusions and Recommendations of the Expert Group

- **The need for Economic incentives** for the relevant industry to achieve that cyber security will be taken into account in the investments for Smart Grids.

- **Revision of the regulatory framework**:
  - Cyber security should be an integrated part of the security process of an electric company.
  - Policy makers need to work with regulatory bodies to establish standards, security guidelines and compliance mechanisms.
  - Tight and contra-productive regulation shall be avoided.

Conclusions and Recommendations of the Expert Group

- **Information sharing (all levels):**
  - Information sharing within and between sectors and the government and determining how to secure and communicate vulnerabilities and attack vectors is key to vendors and end users.

- **Integrity and authenticity of information:**
  - Need for policies that can **guarantee integrity and authenticity of information**.
  - Availability, integrity and authenticity therefore need to be assured across the entire “value chain” of the control signal.

Conclusions and Recommendations of the Expert Group

- **Good practices for cyber security and resilience of the smart grids:**
  - The need for baseline of essential recommendations and requirements to implement the cyber security measures since the earlier stages of the deployment of the smart grid.
  - Need of guidelines and recommendations for the improvement of the cyber security of Industrial Automation and Control Systems (IACS) and Supervisory Control And Data Acquisition (SCADA) systems.

Conclusions and Recommendations of the Expert Group

- **C-Level awareness on cyber security:**
  - The need for raising awareness on cyber security issues among 'decision makers' in Electrical Power organisations/operators .

- **Research & Development for security:**
  - research in risk management, resilience and information security of chains of organisations responsible for the end-to-end supply of energy;
  - research in policy-based incentives to strengthen the end-to-end resilience of the supply of energy and to suppress misbehaviour by high system-based penalties;
  - research and development of architectural security concepts in smart grids, e.g. an N-1 approach equivalent for the ICT-enhanced power grid.

- **Cyber security issues are global and therefore the response has to be global**

Network of initiatives

The Expert Group is also well engaged with EU and international related initiatives: European Task Force Smart Grid (Expert Group 2), CEN/CENELEC/ETSI Smart Grid Information Security (SGIS), EuroScsie (Info Sharing), and

- EU-US ESG on PPP: Cyber security of ICS & Smart Grid
  - **EU-US Joint Open Workshop on Cyber Security of ICS and Smart Grids 15th October 2012, Amsterdam**

European Cyber Security Strategy
Strategic objective

- To be adopted in the third quarter of 2012.
- Aims at ensuring and promoting an open, transparent, secure and resilient global digital ecosystem benefitting EU citizens, businesses and public administrations.
- The strategy will propose measures, including regulatory ones, to ensure a closer cooperation and information exchange between EU public and private stakeholders.

European Cyber Security Strategy
Strategic objective

- Will aim to stimulate private sector efforts to improve security in products and services through the development of appropriate incentives, as well as to put in place appropriate framework conditions for promoting the development of a vibrant EU ICT security industry.

- Opportunities and funding schemes encouraging the deployment of appropriate technological solutions, which respond both to present and future security challenges, will be further put forward in Horizon 2020 and the Connecting Europe Facility.

European Commission

Thanks!

Links to policy documents

- **Commission Communication on Smart Grids "Smart Grids: from innovation to deployment"**

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0202:EN:HTML:NOT

- **Commission Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" - COM(2011) 163**
  http://ec.europa.eu/information_society/policy/nis/docs/comm_2011/comm_163_en.pdf

- **Digital Agenda for Europe - COM(2010)245 of 19 May 2010**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

- **Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids**

  http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2712

Web Sites

EU policy on Critical Information Infrastructure Protection – CIIP
http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

A Digital Agenda for Europe
http://ec.europa.eu/information_society/digital-agenda/index_en.htm

EU policy on promoting a secure Information Society
http://ec.europa.eu/information_society/policy/nis/index_en.htm

European principles and guidelines for Internet resilience and stability
http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf