Cyber security of SMART GRIDS
Commission Policy initiatives-State of play

Alejandro PINTO
European Commission

Trust & Security
DG CONNECT

alejandro.pinto-gonzalez@ec.europa.eu

Main relevant Policies

- **European Programme for Critical Infrastructure Protection (EPCIP) COM(2006) 786, (under revision)**

"..the importance of interdependencies in general, and between ICTs and the energy sector.."

➢ *CIP Expert Group on cross-sectorial interdependencies between the ICT sector and electricity networks (2008)*

- **Digital Agenda (COM(2010) 245) & Action Plan on Critical Information Infrastructures Protection (COM (2009) 149- COM(2011) 163)**
  - ➢ ***Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids (2010)***

- **COM (2011) 202 "Smart Grids: from innovation to deployment"**

  "…the commission will continue bringing together the energy and ICT communities within and expert group to assess the network and information security and resilience of Smart Grids as well as to support related international cooperation"

Expert Group on

Security and Resilience of Communications Networks and Information Systems for Smart Grids

In 2010, the European Commission, with the support of the European Network and Information Security Agency (ENISA), set up 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.**

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

(Full Report in http://ec.europa.eu/information_society/policy/nis/)

- **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.
  - ➢ **ENISA study on minimum security measures for Smart Grids (29 Nov 2012)**
- **Incident management:**
  - Mandate to a governmental authority in charge of responding to incidents and managing crisis due to cyber-attacks on smart grid (power grids).
  - ➢ **(European Strategy for Cyber security)**
- **(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.

- **Security and certification standards:**
  - An EU-wide harmonization of security standards is needed.
  - ➢ **Joint ENISA – European Commission workshop on security certification for smart grid components (27 June 2012)**

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.
  - ➢ **JRC – EG2(Smart Grid Task Force): Evaluating the need and features of a Network for information sharing.**

- **Industrial Control Systems, and not only the smart meters, draw today the primary cyber security focus**.
  - ➢ **ENISA Study on the ICS/SCADA Security**

- **Integrity and authenticity of information:**
  - Need for policies that can **guarantee integrity and authenticity of information (system control)**.
  - 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

- **The need for different levels of security measures** adapted to the different architectural layers of the smart grid, to keep the Smart Grid infrastructure as robust and as resilient as possible.

- **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.
  - ➢ **JRC- EG2: Best available techniques for 10 minimum functional requirements to tackle cyber security.**

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.
  - ➢ **The Grand Conference, Amsterdam 16th October**

- **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**
  - ➢ **EU-US Sub-Working Group on Cyber security of ICS & Smart Grids**
  - ➢ **India, Japan**

Future of work stream on Cyber security of SCADA/Smart Grids

European Strategy for Cyber Security states that:

*"**The Commission**:*
*Will launch a **platform on network and information security solutions** bringing together European public and private stakeholders. The platform will be tasked with the identification and creation of favourable market conditions for the development and adoption of secure ICT solutions. It will also address interdependencies between ICT and critical economic sectors (SCADA/Smart Grids, Transport, etc)."*

- Such **Sub-Group on SCADA/Smart Grids** will follow up the activities of previous CONNECT's Expert Group, it will be a sub-working group on relevant issues. ENISA will support its activities, acting as a technical secretariat, and launching concrete studies according with the Sub-Group work programme.

Thanks

ALEJANDRO PINTO

Alejandro.pinto-gonzalez@ec.europa.eu