# CEER Training on Cyber Security and the Protection of the European Energy Sector

## 12-13 September 2016

### CEER Office, Cours Saint-Michel 30a (5th floor), 1040 Brussels

### *COURSE PROGRAMME*

*Protecting a nation's power system and ensuring reliable supply of energy are top priorities for regulators and governments all around the world.*

*The risk of cyber-attacks in the energy sector is a growing threat, with the potential to disrupt supply to millions of Europe's energy consumers. The issue is therefore moving up the energy regulatory and political agenda. A report by Moody's Investor Services in 2015 identified cyber-attacks in the energy sector as becoming more sophisticated, but national preparedness for such as an event varies greatly.*

*This CEER training course discusses the need for improved cyber security measures to safeguard the European energy sector. It brings together experts with different experiences in cyber security from various sectors within and outside Europe, including energy regulators, telecommunication regulators, the European Commission and the European Network and Information Security Agency (ENISA). The course aims to direct National Regulatory Authorities (NRAs) towards an examination of the state of readiness of their energy market and stakeholders to a cyber-attack. It also aims to identify collaborative solutions to mitigate the risk and impact of cyber-attacks, with the NRAs potentially playing a significant role. It is ideally suited for technical experts as well as high level policy experts who want to get an overview of the policy and legislative developments in cyber security and practical experiences of managing the risks within and outside Europe.*

## Monday, 12 September 2016
## 10:30-17:45

**WELCOME AND INTRODUCTION**

**10:30-10:45** Opening remarks and round-table introduction of the participants

- **Mr Philipp Irschik, Chair CEER Cyber Security Work Stream, E-Control**

**SESSION 1 THE GROWING NEED TO ADDRESS CYBER SECURITY**

**10:45-11:45** EU Policy Context and Legislative Developments: Network and Information Security (NIS) Directive and General Data Protection Regulation

- **Ms Michaela Kollau, European Commission, DG ENER**

**Q&A**

**11:45-12:45** Assessing the emerging threats to the energy sector:

a) Threats
b) Vulnerabilities
c) Attacks
d) Good practices and standards

- **Mr Konstantinos Moulinos, European Network and Information Security Agency (ENISA)**

**Q&A**

*12:45-13:45 Lunch Break*

**13:45-14:30 Case study 1:**

Some examples of cyber events which are relevant for energy regulators

- **Mr Miikka Salonen, Finnish Communications Regulatory Authority (FICORA)/ National Cyber Security Centre Finland (NCSC-FI)**

**Q&A**

**14:30-15:30** Challenges in managing the risks in the energy sector:

a) Roles and responsibilities at the national level
b) Dependency on other sectors
c) New technology threats – smart grid
d) Different government models and different authorities involved
e) Different technologies; gap between IT staff and other experts; poor training at national level
f) Disaster recovery and damage limitation

- **Mr Philipp Irschik, Chair CEER Cyber Security Work Stream, E-Control**

**Q&A**

*15:30-15:45 Coffee break*

**SESSION 2 COLLABORATIVE SOLUTIONS AND THE ROLES OF REGULATORS**

**15:45-17:15 Interactive sessions:**

a) What should NRAs do to protect themselves, including REMIT systems and other sensitive data and information?
b) How should NRAs contribute to improving cyber security in energy markets? Which should be the role of NRAs in enforcing cyber security in energy markets?
c) What regulatory action should be taken within regulated (and possibly unregulated) energy companies?

d) What interdependencies are there with other sectors (water; telecoms; data privacy; retail; ombudsman, etc.)?

- **Moderator: Mr Stefano Bracco, ACER**

**17:15-17:45** Plenary discussion and wrap up of Day 1

- **Mr Philipp Irschik, Chair CEER Cyber Security Work Stream, E-Control**

**19:00-21:00** Dinner – all participants and lecturers are welcome to join (place tbc).

**- END FIRST DAY -**

## Tuesday, 13 September 2016
## 09:00-16:30

**SESSION 3 MANAGING THE RISKS – PRACTICAL EXAMPLES**

**09:00-09:45** Recap of the policy development context and why regulators need to address cyber security. Comparison of the practices from Europe and USA.

- **Mrs Annabelle Lee, Electric Power Research Institute (EPRI)**

**Q&A**

**09:45-10:30 Case study 2:**

How telecommunication and energy actors cooperate on cyber security issues? Practical example from Finland.

- **Mr Miikka Salonen, Finnish Communications Regulatory Authority (FICORA)/ National Cyber Security Centre Finland (NCSC-FI)**

**Q&A**

*10:30-10:45 Coffee break*

**10:45-13:00 Case study 3:**

Simulation exercise of a failure scenario.

- **Mrs Annabelle Lee, Electric Power Research Institute (EPRI)**

**Q&A**

*13:00-14:00 Lunch Break*

**14:00-15:00 Case study 4:**

Private-public partnership initiative to drive cyber-capabilities and resilience collectively in the Austrian energy sector

- **Mr Philipp Irschik, Chair CEER Cyber Security Work Stream, E-Control**

**Q&A**

*15:00-15:15 Coffee break*

**15:15-16:15 Case study 5:** Cyber security measures for smart grids

a) Smart grids: new technologies – new potential avenues of attack
b) Smart grid threat – can a base line level of remedy be set, given so many stakeholders?

- **Mr Paul Smith, Austrian Institute of Technology, SPARKS-Project Coordinator**

**Q&A**

**16:15-16:30** Wrap-up of Day 2

- **Mr Philipp Irschik, Chair CEER Cyber Security Work Stream, E-Control**

**- END SECOND DAY -**