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

12-13 June 2017

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

Module 1: Legal and Policy Developments in Cyber Security – 12 June 2017

Module 2: Risk Management and Preparedness in Cyber Security – 13 June 2017

COURSE PROGRAMME

Throughout the world, countries are increasingly facing cyber security threats and challenges. According to a report of the World Energy Council in 2016, 80% of oil and gas companies saw an increase in the number of successful cyber-attacks in 2015. The energy sector is undergoing substantial changes in infrastructure, in the structure of the markets and in cyber security. With evolving cyber threats, our infrastructure is increasingly vulnerable to disruptive or destructive attacks. Though beneficial to both industries and end users, the introduction of advanced technology and modernization to power systems also introduces a whole new set of vulnerabilities that can be exploited by cyber-attacks.

Regulators must prepare for this new reality by understanding their roles and responsibilities and by taking the necessary steps to improve cyber preparedness of utilities. As regulators are tasked with evaluating the investments of utilities, approving tariffs and ensuring the resiliency and reliability of the grid, it is critical for regulators to understand not only all the dimensions of cyber security, but also the best methods to tackle this issue from a regulatory perspective.

This CEER training course aims to provide policy as well as technical experts from National Regulatory Authorities and National Competent Authorities with an overview of the policy and legislative developments in cyber security and practical experiences on the technical aspects of risk management and preparedness in Europe.

The course comprises of two standalone - but related – modules. Attendance at both modules is recommended, though they are designed such that participants can gain value by attending just one module if they wish. Module 1 is ideally suited for policy experts who want to understand the main challenges and the policy and legislative developments in cyber security within and outside Europe. Technical experts might benefit from attending this module as well. Module 2 is suited for technical experts who want to exchange practical experiences on the technical aspects of risk management and preparedness in cyber security for energy.

Module 1: Legal and Policy Developments in Cyber Security

Monday, 12 June 2017
10:30-17:45

WELCOME AND INTRODUCTION

10:30-10:45 Opening remarks and round-table introduction of the participants of Module 1.

- **Mr Roman Picard, Co-Chair CEER Cyber Security Work Stream, CRE**

10:45-11:30 World guided tour in cyber security for energy: examples of cyber-attacks and their consequences, strategies, approaches and regulations worldwide.

- **Mr Stefano Bracco, Chair CEER Cyber Security Work Stream, ACER**

Q&A/Discussion

11:30-12:15 European Legal Framework: Network and Information Security (NIS) Directive and General Data Protection Regulation.

- **Ms Marie-Theres Holzleitner, Energy Institute at the Johannes Kepler University Linz**

Q&A/Discussion

12:15-13:00 Cyber security - a cross-sector regulation where the energy sector is key. Perspectives from the NIS Directive and Clean Energy Package.

- **Mr Manuel Sanchez-Jimenez, European Commission, DG ENER**

Q&A/Discussion

13:00-14:00 Lunch Break

14:00-14:45 Overview of current actions of DG ENERGY: expert working group and analysis of risks and costs of preventing cyber-incidents in the energy sector.

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

Q&A/Discussion

14:45-15:45 How is NIS implemented in EU? Recent developments on incident reporting, security measures and identification criteria for operators of essential services.

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

Q&A/Discussion

15:45-16:00 Coffee break

16:00-16:45 Experience from Austrian Energy Computer Emergency Response Team (CERT) – the first sectoral Computer Security Incidents Response Team (CSIRT) in Austria.

- **Mr Stefan Lenzhofer, Austrian Energy CERT (AEC)**

Q&A/Discussion

16:45-17:30 Regulating cyber security in non-EU Countries: lessons learned, issues and limits of a regulation to tackle a threat without national boundaries.

- **Mr Rajesh Nair, Detecon**

Q&A/Discussion

17:30-17:45 Final remarks and wrap up of Module 1

- **Mr Roman Picard, Co-Chair CEER Cyber Security Work Stream, CRE**

17:45-18:45 Reception drinks – For those who wish to join, we will host a small drinks reception at the CEER office – all participants and lecturers welcome!

- END OF MODULE 1 -

Module 2: Risk Management and Preparedness in Cyber Security

Tuesday, 13 June 2017
09:00-16:45

09:00-09:10 Opening remarks and round-table introduction of the participants of Module 2.

- **Mr Roman Picard, Co-Chair CEER Cyber Security Work Stream, CRE**

09:10-10:00 10 risks of cyber: detection, prevention and mitigation.

- **Mr Stefano Bracco, Chair CEER Cyber Security Work Stream, ACER**

Q&A/Discussion

10:00-11:15 Smart meters and smart grids: to which risks are they exposed? The future of cyber security for the grid.

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

Q&A/Discussion

11:15-11:30 Coffee break

11:30-12:15 Experience on the rolling out of advanced metering infrastructures in EU and it impacts on cyber security.

- **Mr Wolfgang Löw, EVN AG**

Q&A/Discussion

12:15-13:00 Building a cyber security scenario and testing them on the ground: how an exercise can foster preparedness.

- **Mr Alexandros Zacharis, European Network and Information Security Agency (ENISA)**

Q&A/Discussion

13:00-14:00 Lunch Break

14:00-14:45 What are the Best Available Techniques (BATs) in cyber security?

- **Mr Igor Nai-Fovino, European Commission, DG JRC**

Q&A/Discussion

14:45-15:30 Distributed Ledger Technologies: role, technologies behind, risks and future use.

- **Mr Igor Nai-Fovino, European Commission, DG JRC**

Q&A/Discussion

15:30-15:45 Coffee break

15:45-16:30 Cyber security standards - Why using them, which and how? A reasoned analysis of available possibilities.

- **Mr Roman Picard, Co-Chair CEER Cyber Security Work Stream, CRE**

Q&A/Discussion

16:30-16:45 Final remarks and wrap up of Module 2

- **Mr Roman Picard, Co-Chair CEER Cyber Security Work Stream, CRE**

- END OF MODULE 2 -