EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY

Directorate B - Internal Energy Market
B.3 - Retail markets; coal & oil

Energy Expert Cyber Security Platform (EECSP)
Terms of Reference (EECSP) & Call for Experts (EESCP-Expert Group)

1. Introduction

Ensuring resilience of the energy supply system against cyber-threats will be increasingly important as wide-spread use of IT and data traffic become the foundation for the functioning of infrastructures underlying the energy system. Energy infrastructure is arguably one of the most complex and critical infrastructure that other sectors depend upon to deliver essential services. An ever smarter energy system can perform power generation, transmission, network management and marketing related tasks with much better precision and faster response times than human-dependent systems, thereby saving energy, prioritizing usage, and setting policies for quick response to outages. However, this increased efficiency in supply services comes with a price: increased exposure to cyber-attacks with the potential to impair:

- *Confidentiality* – unauthorized access to or interception of information.
- *Integrity* – unauthorized modification of information, software, physical assets.
- *Availability* – blockage of data transmission and/or making systems unavailable.

These threats apply to all generation, transmission and distribution technologies, and to energy market services. Recognising this new situation, Commission services (Commission's Directorate-General for energy (hereinafter 'DG ENER') in lead) aim to create an expert platform on cyber security to cover all cyber threats impacting the energy sector.

2. Policy context

The forthcoming NIS Directive[1] and the forthcoming General Data Protection Regulation[2] (GDPR) will create a new generic framework for handling cybersecurity in the EU. Furthermore, the European Agenda on Security 2015-2020[3] adopted in April 2015 and the Digital Single Market Communication of 6 May 2015 stressed the need for a common approach to address cyber threats across Europe[4] building on the existing EU cybersecurity strategy launched in 2013[5].

Thus a comprehensive energy-sector strategy on cyber security could reinforce the implementation of the forthcoming NIS directive at energy sector level and also foster synergies between the Energy Union and the Digital Single Market agenda.

1http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and

2 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[3] COM(2015) 185 final

[4] COM (2015) 192 final (pp. 13, 20) and the accompanying SWD (2015) 100 final (pp. 47-51).

[5] The Strategy of the European Union[5] set up in 2013 a public-private cross-sectoral platform on Network and Information Security (NIS Platform)[5] to contribute to Commission recommendations on good cybersecurity practices, in particular on risk management, information sharing and incident notification.

Building upon work previously carried out by the Commission, DG ENER will set up and coordinate a process to define a full-sector strategy on cyber security in energy, in cooperation with other Commission services. The strategy could lead on one hand to formal adoption of sectoral instruments, e.g. through EC Recommendations or implementing acts under the forthcoming NIS Directive and/or General Data Protection Regulation, and on the other hand should kick-start a continuous process of sharing good practices in the energy sector through regular evaluation and reporting which could also feed into future Energy Union legislative and non-legislative initiatives, if and as appropriate.

3. Organisation of the EECSP

The EECSP activities are structured as the following:

- The EECSP-Expert Group (see point 3.1.)
  - an informal and temporary Commission expert group
- The EECSP-Forum (see Annex 1)
  - annual conferences on top of the EECSP-Expert Group with open participation

3.1. EECSP-Expert Group

3.1.1. Mission and duties of the EECSP-Expert Group

- The mission of the EECSP-Expert Group (hereinafter also called 'the expert group') is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies as well as nuclear.
- The first deliverable of the EECSP-Expert Group is to analyse existing legislation, initiatives, projects and cyber security strategies related to all parts of the energy sector in order to pinpoint areas where a sectoral approach is needed. For example, the EECSP-Expert Group will suggest concrete modalities for the risk management and incident notification obligations as expected to be required under the NIS Directive. The EECSP-Expert Group will also analyse the interplay between various EU legislative instruments applicable to the energy sector, e.g. the NIS Directive and the General Data Protection Regulation, ways to streamline the corresponding obligations impacting the energy sector as well as indicate specific solutions. An initial mapping is scheduled in the roadmap table (see Annex 2).
- The second deliverable is to develop a short-, medium-, and long term strategy building on the first deliverable and to reinforce the implementation of the new legal basis of the forthcoming NIS directive and the GDPR and to provide input for future legislative acts to be adopted in future.
- The third deliverable will involve regular monitoring of the various findings in line with the implementation of relevant legislation and the evolution of risks, threats and vulnerabilities in the energy sector.

3.1.2. Membership and operation of the EECSP-Expert Group

The expert group will be composed of up to maximum 15 experts.

Members of the group will be designated in accordance with the Commission rules on expert groups[6]. More specifically they may be:

[6] Commission Communication establishing the Framework for Commission Expert Groups (C(2010) 7649 / SEC(2010) 1360)

- (a) individuals appointed in their personal capacity – i.e. experts with outstanding knowledge in their areas acting independently and in the public interest, who cannot represent any specific interest nor being affiliated with private organisations which may benefit from the work of the group;

- (b) individuals appointed to represent a common interest shared by stakeholders in a particular policy area; they shall not represent an individual stakeholder.

Members must be nationals of a Member State of the European Union or, of an acceding country or a European Economic Area country or a state which has signed an association agreement or a third country.

When defining the composition of the group, the Commission shall aim at ensuring a balanced representation of relevant areas of expertise and areas of interest, as well as a balanced representation of gender and geographical origin, while taking into account the specific tasks to be carried out by the group and the type of expertise required.

The mandate for the expert group will be limited to 2 years with the possibility of prolongation. DG ENER will chair and provide secretariat for the expert group.

The expert group will meet periodically. Within the first six months three meetings are foreseen, with the possibility to in-/decrease depending on necessity. Please see the scheduled roadmap (Annex 2) for further details. After the first six months the expert group will meet on a quarterly basis. Depending on the needs of the expert group additional meetings might be hold.

The group may set up sub-groups to examine specific questions on the basis of terms of reference defined by the group. Such sub-groups shall be disbanded as soon as their mandate is fulfilled.

Members of expert groups and their representatives, as well as invited experts and observers, shall comply with the obligations of professional secrecy laid down by the Treaties and their implementing rules, as well as with the Commission's rules on security regarding the protection of EU classified information, laid down in the Annex to Decision 2001/844/EC, ECSC, Euratom. Should they fail to respect those obligations, the Commission may take all appropriate measures.

The group's deliberations shall be confidential. In agreement with the Commission's services, the group may, by a simple majority of its members, decide to open its deliberations to the public.

If sensitive but unclassified information is to be shared among members, the Traffic Light Protocol (TLP) shall be used (see annex 3). This is without prejudice to provisions on transparency included under paragraph 3.1.6.

3.1.3. Selection Criteria of the EECSP-Expert Group

Regardless of whether applications are made as individuals to be appointed in a personal capacity or individuals representing a common interest, DG ENER expects that the background, expertise, experience and level of seniority of the applications will be commensurate with the high prominence of advisory tasks assigned to the EECSP – Expert Group.

In particular, the Commission will take the following criteria into account when assessing applications:

- High degree and recognition of expertise and, for individuals referred to in paragraph 3.1.2 (b), the capacity to represent relevant stakeholders operating in a given policy area.
- Substantial accumulated experience in activities in the interdisciplinary domain of ICT for Energy at EU level.
- High level in the organisation which should have significant involvement in the EECSP related activities.
- Access to authoritative experts of international standing involved in a wide range of activities relevant to the EECSP activities.
- High degree of commitment to the EECSP-Expert Group and the ability to devote sufficient time and resources to its activities.
- Substantial accumulated experiences in energy (covering oil, gas and electricity including nuclear) as well as in the use of ICT and its application in the energy sector. Experience with dealing with cyber security aspects of ICT use will be preferred.
- Adequate knowledge of the English language allowing applicants to participate actively in the discussions within the EECSP and the drafting of documents.

3.1.4. Application procedure

Each application may be completed in one of the official languages of the European Union. However, applications in English are encouraged as they facilitate the evaluation procedure. If another language is used, it would be desirable to include a summary of the CV in English.

Applicants must clearly indicate whether the application is made for an individual in their personal capacity or an individual appointed to represent a common interest shared by stakeholders.

Applications must also include an informative overview of the applicant's professional experience and expertise by means of a curriculum vitae and a letter in support of their application.

Each application should include the following information (not exhaustive) in his/her CV and Letter of Motivation:

- In which capacity the application is being made (individual to be appointed in a personal capacity or to represent a common interest)
- The name and profile of the applicant
- For individuals representing a common interest a brief description of which interests are represented (representativeness)
- The authority/organisation for which the applicant has been working and the length of time he/she has worked there
- Other authorities/organisations, for which he/she has worked in the past
- His/her specific competences including language skills
- The specific projects and or tasks he/she has been involved in
- Any works that he/she has published
- Any experience he/she has acquired at EU and international level
- His/her major professional challenges foreseen in the near future
- For individuals to be appointed in a personal capacity, any interests that he/she has, which may prejudice his or her independence
- Confirmation to allow adequate time and resources to advice the Commission

3.1.5. Deadline for application

The application should be sent no later than 30 September 2015 via e-mail to the address ENER-B3-EECSP@ec.europa.eu. The date of the e-mail will be the date of sending.

3.1.6. Transparency

The members' name will be collected, processed and published in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[7].

The names of members shall be published on the internet site of the Directorate-General for Energy and in the Register of Commission Expert Groups (hereinafter 'the Register') and other similar entities in accordance Commission rules on expert groups[8].

All relevant documents (such as agendas, minutes and participants' submissions) shall be made available in the Register or via a link from the Register to a dedicated website where information can be found. Exceptions to publication are justified where disclosure of a document would undermine the protection of a public or private interest as defined in Article 4 of Regulation (EC) N° 1049/2001. See also point 3.1.2.

3.1.7. Logistical and operational aspects

The EECSP-Expert Group shall meet in Brussels on Commission premises or in another place announced in accordance with the procedures and schedule established by the Commission.

Travel expenses incurred by participants in the activities of the EECSP-Expert Group shall be reimbursed by the Commission in accordance with the provisions in force at the Commission within the limits of the available budgetary appropriations. Participants in the activities of the EECSP-Expert Group shall not be remunerated for their duties.

[7] OJ L 8, 12.1.2001, p. 1.

[8] Commission Communication establishing the Framework for Commission Expert Groups (C(2010) 7649 / SEC(2010) 1360)

4. ANNEX 1: The EECSP-Forum

The meetings of the EECSP-Expert Group will be complemented by the EECSP-Forum which meets at least once a year in form of a conference. The Forum aims to monitor the progress achieved within the Expert Group meetings, steer their activity towards most desirable/useful outcomes from the energy sector perspective, and to validate the sector-wide relevance and applicability of the Expert Group outputs. Periodical reporting to NIS Platform could be proposed in order to reinforce coherence with general NIS principles.

Additional to the experts of the EECSP-Expert Group, Member States' authorities in charge of cyber security issues in the energy sector as well as interested organisations, in the broad sense of the word including companies, associations, Non-Governmental-Organisations, trade unions, universities, research institutes, Union agencies, Union bodies and international organisations are welcome to contribute to the EECSP-Forum meetings.

See below an indicative but non-exclusive list of possible participants in the EECSP-Forum are EU-wide associations from:

- Electricity and Gas Transmission and Distribution system operators
- Oil infrastructure (crude oil and petroleum products pipelines) operators
- Energy generators and industrial associations
- Suppliers of automation and control systems and associated technologies
- Energy trading entities
- ACER/CEER
- Providers of services and products of information and communication technologies in the energy sector
- Energy Community Secretariat
- ESARDA (European Safeguards Research and Development Association)
- FORATOM (Forum of European Nuclear Associations)

The EECSP-Expert Group will help the European Commission to organise the EECSP-Forum.

To inform the EECSP-Forum in between conferences, an EECSP-Forum web portal will be created to facilitate consistent communication.

5. ANNEX 2: Roadmap

Action Description	Start date	End date	Deliverables
Select experts	30/09/2015	16/10/2015	EC to select experts
1st Meeting EECSP-Expert Group	29/10/2015	29/10/2015	1st Expert Meeting
Deliverable 1: Analysing existing legislation, initiatives, projects and cyber security strategies related to all parts of the energy sector in order to pinpoint areas where a sectoral approach is needed. More specifically, the EECSP Expert Group will suggest concrete modalities for example the risk management and incident notification obligations as set out under the framework of the Commission proposal for the NIS Directive. The EECSP Expert Group will also analyse the interplay between various EU legislative instruments, e.g. the NIS Directive and the Data Protection Regulation, ways to streamline the corresponding obligations impacting the energy sector as well as indicate specific solutions. The draft deliverable will be reviewed by ENISA to ensure completeness and relevance.	29/10/2015	16/12/2015	Draft Report 1st part deliverable 1
2nd Meeting EECSP-Expert Group- discussion of analysis and draft report	16/12/2015	16/12/2015	2nd Expert Meeting
1st Meeting EECSP-Forum: Official launch of expert platform	17/12/2015	17/12/2015	Meeting with Experts & Stakeholders
Deliverable 1: Finalisation	17/12/2015	15/03/2016	Draft Report 2nd part deliverable 1
3rd Meeting EECSP-Expert Group - Finalisation of first deliverable and start of second deliverable (short-, medium- an long term strategy)	15/03/2016	15/03/2016	3rd Expert Meeting/Final report Deliverable 1 **END OF DELIVERABLE 1**
Deliverable 2: Analysis short-, medium- and long term strategy building on the first deliverable and to reinforce the implementation of the new legal basis of the forthcoming NIS directive and the GDPR and to provide input for future legislative acts to be adopted in future.	15/03/2016	21/06/2016	Draft report
4th Meeting EECSP-Expert Group: Short-, medium- an long term strategy	22/06/2016	22/06/2016	4th Expert Meeting
2nd Meeting EECSP-Forum: Cyber Security Conference, Main topic will be the Cyber Security Strategy, with the input of the broader stakeholders group.	23/06/2016	23/06/2016	Meeting with Experts & Stakeholders
Drafting Cyber Security Strategy (adhoc meetings, telcos)	23/06/2016	27/10/2016	First draft Deliverable 2
5th Meeting EECSP-Expert Group: Finalisation Short-, medium- an long term strategy	27/10/2016	27/10/2016	5th Expert Meeting
3rd Meeting EECSP-Forum: Conference on Implementation of Cyber Strategy	Oct/Nov 2016	Oct/Nov 2016	Meeting with Experts & Stakeholders
Finalisation Deliverable 2: Cyber Security Strategy	27/10/2016	25/11/2016	Final Strategy **END OF DELIVERABLE 2**
Commission will assess potential policy requirements	Q4 2016	Q1 2017	Recommendations for Sectoral Measures
Deliverable 3: will involve regular monitoring of the various findings in line with the implementation of relevant legislation and the evolution of risks, threats and vulnerabilities in the energy sector.	Q4 2016	-	regular monitoring, quarterly meetings

Remark: Timing might adjust regarding the process of the negotiations of the NIS directive. EECSP-Forum Meetings are subject to change due to room and personal availability.

6. ANNEX 3: The Traffic light Protocol[9]

The Traffic Light Protocol (TLP) was created by the UK Centre for the Protection of National Infrastructure (CPNI) in order to encourage greater sharing of information. Information sharing is important for helping mitigate the spread of electronic attacks, improving protection through sharing best practices, and building trust between players in this field. In order to encourage the sharing of sensitive (but unclassified) information, however, the originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all.

The TLP provides a simple method to achieve this. It is designed to improve the flow of information between individuals, organisations or communities in a controlled and trusted way. It is important that everyone understands and obeys the rules of the protocol.

Only then can trust be established and the benefits of information sharing realised.

The TLP is based on the concept of the originator labelling information with one of four colours to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

The four colours and their meanings are:

RED — Personal for named recipients only

In the context of a meeting, for example, **RED** information is limited to those present at the meeting. In most circumstances, **RED** information will be passed verbally or in person.

AMBER — Limited distribution

The recipient may share **AMBER** information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.

GREEN — Community wide

Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community.

WHITE — Unlimited

Subject to standard copyright rules, **WHITE** information may be distributed freely, without restriction.

[9] See Annex of : http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=2377&no=1