Terms of Reference for the ENISA NCSS Working Group

1 Background

Studies have shown that cyber security incidents can have a great societal impact. Now more than ever, Member States need to be prepared to address and respond to cyber threats. 22 out of the 28 Member States already have a National Cyber Security Strategy (NCSS), and others are in the process of drafting one with the intend to achieve and maintain a high level of security of their network and information systems. With the agreement on the NIS directive, all Member States should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented

ENISA has been dealing with NCSS since 2011. ENISA's role is to assist, support and advice the Member States on Network and Information Security matters. This is done through studies that result into specific recommendations, events and conferences that raise awareness, and formation of expert groups, that bring together the community.

ENISA started working on the NCSS in 2011 and published the first deliverable with an analysis on the status of National Cyber Security Strategies in the Member States and in the world. With the objective to assist Member States in the development, implementation and evaluation of a NCSS, ENISA developed in 2012 a NCSS Implementation Guide with information about the NCSS lifecycle and concrete actions and steps, which if implemented will lead to a coherent and holistic national cyber security strategy. An evaluation framework for NCSS has also been developed in 2014 with a set of steps and KPIs to help stakeholders to map their objectives in an evaluation model. Moreover, ENISA has created a repository with a list of the developed NCSS in Europe and worldwide together with an interactive map. An e-learning platform which was launched in 2016 with the aim to provide interactive training courses in regards the several stages of designing, implementing and evaluating a NCSS is a sample of ENISA's work in the area.

2 Objectives

The NCSS Working Group brings together Member States' public officials and policy makers that usually lead the process of developing and implement cyber security strategies. This group provides ENISA with the opportunity to listen to suggestions and ideas. The group constitutes an exchange platform for the participants to address important issues relating to national cyber security and resilience of national and international systems and infrastructures.

Your role in the experts group would be:

- To share your knowledge and experience with ENISA and to have your view reflected in relevant position papers on NCSS topics and validate information,
- To participate (give presentations, participate in panels etc) in workshops or other related events regarding NCSS,
- and to directly discuss within the group the approaches other MS are taking towards NCSS.

The benefits you will gain are:

- your knowledge and expertise will be included in documents that are widely open to the wide European (and not only) community, and taken into account by policy makers, CII operators, regulators, etc.
- the good practices you follow can lead the example and assist other Member States to fill gaps in their NCSS,

- you will become part of the ENISA community ecosystem which involves only experts on the field and creates trends in cyber security in the EU.

3 NCSS Stakeholder Group Members

Member of the Experts Group can be:

1. Individuals appointed in their personal capacity.
2. Individuals appointed to represent a common interest shared by stakeholders in a particular policy area; they shall not represent an individual stakeholder.
3. Organisations in the broad sense including companies, associations, governmental and non-governmental organisations, universities, research institutes, European Union Agencies and Bodies, international organisations.

Involved individuals are selected based on excellence in the following skills (indicatively):

- Excellent understanding of policy and regulatory issues related to the security of Internet at national and/or pan European level including activities related to Critical Information Infrastructure Protection (CIIP);
- Knowledge of CIIP and cyber security strategy and policy at national and/or pan European level;
- Experience and/or good understanding of cyber security;
- Experience from interaction with relevant stakeholders/users;
- Active participation in other relevant communities.

The working language is English.

In addition to the above mentioned skills, the review of applications also take into account the following criteria:

- Individuals are appointed to represent a common interest shared by the type of stakeholders; as such they do not represent an individual stakeholder;
- The formation of the group will be done in a way that a mix of skills in the area of security and resilience of systems and infrastructures, geographic coverage is taken into account;
- Limited number of experts in order to efficiently interact in achieving desired outcomes; (maximum 35 members and 5 alternate members);
- Interest or motivation of the Expert to the policy and CIIP area;
- General background of the Expert in the policy and CIIP area;
- Gender balance.

4 Administrative information

4.1 Approach/ Working Methods

The structure of the reference group is organized around periodic conferences calls, mailing list and a space on the resilience portal website. Members will be asked to provide input on ENISA work in the area and highlight trends and current operational issues. In addition to the contribution of the Experts Group to the collection of

requirements and ideas, the group will contribute to the review of ENISA deliverables of related projects. Experts will be acknowledged in the ENISA reports as contributors.

The main means of interaction will be online tools (web conferencing, mails, and phone) and the dedicated portal. One physical meeting could be held once a year. The arrangements of this meeting are going to be discussed and agreed with the group members.

4.2 Organisational modalities

A long term commitment by the group members is desirable. The contribution of each member of the NCSS Working Group is roughly estimated with ca. 2 person days per year. This engagement does not include the time required for a potential physical meeting.

The effort of members invested in the NCSS Working Group activities will not be reimbursed by ENISA.

The travelling expenses of NCSS Working Group related to a potential physical meeting will not be reimbursed. ENISA is going to facilitate the organisation of a possible meeting by means of the meeting venue and catering.

From each conference call and meeting, short result oriented minutes will be drafted and sent for approval to the NCSS Working Group members.

4.3 Data protection

Personal data of participants in Informal Expert Groups will be processed 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.

4.4 Transparency

The members and Chair of the reference group are subject to the requirement of confidentiality pursuant to article 287 of the Treaty for the Functioning of the European Union, even after their duties have ceased. In particular without prejudice to the provisions of Regulation (EC) No. 45/2001, they shall be required not to disclose information of the kind covered by the obligation of professional secrecy, such as information about undertakings, their business relations or their cost components, as well as information relating to the investigation of criminal offences and the application of criminal law.