

The Hague, 23/05/2013



## **Terms of Reference and mandate of the Advisory Group on Internet Security**

### **1. Status**

---

The Advisory Group on Internet Security (hereafter 'the Group') is an advisory group to the Programme Board of the European Cybercrime Centre (EC3), established by and reporting to the Programme Board of EC3 (hereafter 'The Programme Board').

The Group is set up for an initial period of two years. Its work will then be subject to review by the Programme Board, which may decide to extend its term for another two years.

The Head of EC3 will appoint the Chair of the Group after consulting with the members of the Programme Board. The EC3 will act as the Secretariat to the Group.

The Chair need not be member of the Programme Board, but as far as possible should receive endorsement by Programme Board consensus concerning their suitability. Individual nominations to chair will be subject to the same level of scrutiny as applications for membership (see below).

In terms of deliverables and performance monitoring, the Groups will report in writing at least twice a year in line with the mandate defined by the Programme Board. The Chair and the Group will deliver regular oral updates at the Programme Board.

### **2. Tasks and role**

---

With a view of getting a clear overview of the needs and priorities for internet security in the context of the fight against cybercrime, the purpose of the Group is to:

- bring knowledge and expertise to the Programme Board on matters related to internet security;
- update and share all relevant information and expertise on developments in the area of internet security;
- assist the Programme Board in defining priorities for the work of EC3 in this area, including by advising on the cooperation with CERTs and other relevant partners and on developing concepts for enhanced prevention;
- assist the EC3 Programme Board in striking the right balance between disruption and prevention on the one hand and investigation and prosecution on the other hand.

The Programme Board may also consult the group on any matter relating to internet security in relation to the fight against cybercrime.

## **Europol Unclassified – Basic Protection Level**

### **Releasable to the EC3 Programme Board**

The Programme Board has the option to assign specific tasks and deliverables to the group.

### **3. Membership**

---

In principle, the group shall be composed of up to 12 members representing a wide-range of expertise in all the aspects of internet security, including from the CERT community related to the fight against cybercrime and also a balanced representation in terms of background and geographic regions. The Programme Board will determine the exact number of members, taking into account the need to ensure balanced representation of the various groups and fields of expertise while ensuring that the Group can function in an effective manner.

Members shall be individuals of proven expertise and professional experience in internet security areas which are relevant to the fight against cybercrime. Envisaged in this respect are in particular professionals from the ICT Security/anti-virus industry and CERTs. Furthermore, also law enforcement experts in this crime area are required to complement the discussions from the law enforcement angle.

Members shall be appointed by the Chair of the Programme Board from among those who have responded to the call for applications (see Annex to the present Terms of reference).

On the basis of the call for applications, applicants who were deemed suitable candidates for group membership but were not appointed shall be placed on reserve list, with their consent. The Programme Board shall use this list for the appointment of replacements for members, if needed. If the Programme Board considers the reserve list insufficient, it may re-publish the call for applications in order to constitute a new list.

Members shall be appointed in a personal capacity for a period of two years. They shall act independently – in the sense that they represent their sector and not their individual corporate entity – and in the public interest. They shall remain in office until replaced or until their term of office ends. Their term of office may be renewed.

Members who are no longer capable of contributing effectively to the group's deliberations, who resign or who do not comply with the conditions set out in this Article may be replaced for the remainder of their term of office.

The names of the group's members shall be published on the EC3's website.

### **4. Meetings**

---

Meetings of the Group shall be convened at least twice per year, either virtually or offline. As far as possible, offline meetings of the Group should be scheduled back-to-back with other meetings on related topics or in which several members of the Group are expected to participate. Additional meetings may also be organised on an ad hoc basis when necessary.

As the Secretariat, EC3 will be responsible for invitation, agendas, proposals, minutes and drafting a yearly activity report to the Programme Board. The deliverables of the Group will be submitted to the Programme Board of EC3. The chair of the Group will also provide oral reports to the Programme Board

## **Europol Unclassified – Basic Protection Level**

### **Releasable to the EC3 Programme Board**

drawn from the minutes of the Group's meetings. A draft agenda will be circulated at least two weeks in advance of the meetings of the group in order to allow Members to suggest changes and additions.

Participants in the activities of the group shall not be remunerated for the services they render.

Financial support for travel expenses in connection to meetings may be granted, subject to available funding in the EC3 budget – requests for financial assistance should be made to the Programme Board via the Chair of the Group. In principle, only representatives of public bodies and civil society organisations shall be entitled to receive financial support.

## **5. Areas of work for 2013-2014**

---

In 2013 and 2014, the activity of the Group will focus on the following sub-areas:

- Elaborate and propose a concrete cooperation model to organise the coordination between law enforcement, CERTs, ICT Security/anti-virus industry and other relevant partners in the enforcement and strengthening of cyber security;
- Prepare a proposal for the EC3 Programme Board of a coherent set of criteria that structure the decision making on tackling concrete cyber security threats in such a way that both preventive and investigative interests will be balanced under all circumstances;
- In anticipation of the new data protection regulation, elaborate what kind of information can be shared/exchanged between CERTs, ICT Security/anti-virus industry and law enforcement and under which conditions;
- Define specific suggestions for pilot projects for operational cooperation between law enforcement, ICT Security/anti-virus industry and CERTs.

The Group may contribute to the definition of their areas of work by providing the Programme Board with suggestions on topics where the Group may provide useful guidance or expertise.

## **6. Documents**

---

The Group's Secretariat will make documents available to the members via a dedicated page on the restricted EC3 SPACE website and through e-mail communication as appropriate. Programme Board members will have access to Group's documents.

The Programme Board encourages the use of the virtual platform EC3 SPACE to ensure a constant exchange of information between Work Stream and Advisory Group members.

The Programme Board can authorise public access to a document of the Group, after the document has been discussed by the Group and if no member has explicitly requested confidentiality; requests for confidentiality will be included into the minutes of the meetings.

## **7. Confidentiality**

---

Members of Advisory Groups are free to refer to their membership in the public domain, but must treat the content of meetings, the groups' activities and related documentation as confidential. The Programme Board reserves the right to dismiss any member of an Advisory Groups who is identified as using his or her membership for undue influence, including commercial advantage.

No exchange of data containing crime related personal information will take place during the meetings of the Advisory Groups.

## **8. Review of the Terms of Reference**

---

These Terms of Reference will be presented to the Programme Board for review at the end of every year or whenever the need arises.

## **Europol Unclassified – Basic Protection Level**

### **Releasable to the EC3 Programme Board**

#### ANNEX

### **Call for applications for the selection of Members of the Advisory Group on internet security of the Programme Board of the European Cybercrime Centre appointed in a personal capacity**

On 28 March 2012 the European Commission proposed to establish the European Cybercrime Centre (EC3) at Europol . This proposal was endorsed by the Council of the European Union in June 2012 .

In response to the Commission's recommendations, an EC3 Programme Board has been established within the existing governance structure of Europol, and chaired by the Head of EC3. The Programme Board has identified the need for establishing collaborative work streams and advisory groups on a number of key issues and deliverables.

The tasks of the Advisory Group are:

- bring knowledge and expertise to the Programme Board on matters related to internet security;
- update and share all relevant information and expertise on developments in the area of internet security;
- assist the Programme Board in defining priorities for the work of EC3 in this area, including by advising on the cooperation with CERTs, ICT Security/anti-virus industry and other relevant partners and on developing concepts for enhanced prevention;
- assist the EC3 Programme Board in striking the right balance between disruption and prevention on the one hand and investigation and prosecution on the other hand.

The Programme Board may also consult the group on any matter relating to internet security in relation to the fight against cybercrime.

The Programme Board has the option to assign specific tasks and deliverables to the group.

The Programme Board of EC3 is therefore calling for applications with a view to selecting members of the Advisory Group.

The Advisory Group shall consist of up to 12 members appointed in their personal capacity.

The Chair of the Programme Board shall appoint members in a personal capacity for a two-year renewable period. They shall give the Advisory Group an independent opinion free from outside influence and respect the conditions of confidentiality set out in the Advisory Group's terms of reference. They shall undertake to act independently and in the public interest.

The Programme Board will take the following criteria into account when assessing applications:

- (a) proven competence, and a high level of professional achievement and experience (at least five years), including at European and/or international level, in activities concerned with internet security related to the fight against cybercrime;
- (b) demonstrated ability to work in English;
- (c) the need to strike a balance within the group of experts in terms of institutional and professional background, gender and geographical origin;

## **Europol Unclassified – Basic Protection Level**

### **Releasable to the EC3 Programme Board**

(d) the need to ensure the required balance of expertise required on all internet security matters, and the various aspects involved, such as but not limited to the development of projects and products, supervision or contribution to the research activities of public or private entities, assessment of use and needs for new products and services by the law enforcement community.

The above will be assessed on the basis of the filled-in completed curriculum vitae (CV) and the application form.

Applications may only be submitted using the model application form and should be accompanied by a CV. Applicants are asked to state clearly in their application the industrial area in which they possess particular expertise.

The applications must be sent in 20 working days from the date of publication of the call for applicants, either by e-mail or by post, to the following address: [O3@europol.europa.eu](mailto:O3@europol.europa.eu) or

EC3 – European Cyber Crime Centre  
c/o Europol  
P.O. Box 908 50  
2509 LW - The Hague  
The Netherlands

Where applications are sent by e-mail, the date of e-mail will be the date of sending. Where applications are sent by post, the postmark will be considered the date of sending.

Personal data will be processed in accordance with the principles of 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. These principles of Regulation (EC) No 45/2001 are laid down in the relevant decision of the Europol Director.

The application form and the Terms of Reference for the Advisory Groups are available on EC3 SPACE and on the Europol website under EC3. For any further information please contact the Programme Board Secretariat e-mail: [O3@europol.europa.eu](mailto:O3@europol.europa.eu).

Information on the results of the call for applications will be published on EC3 SPACE and on the Europol website under EC3.