Terms of Reference - ENISA Article 13a Expert Group

1 Introduction and background

The ENISA Article 13a Expert Group was formed in 2010 to facilitate a process of voluntary and informal collaboration between experts of NRAs from across the EU, to discuss and agree on the implementation details of Article 13a of the Framework directive, which regards security requirements for providers of electronic communications networks and services.

The ENISA Article 13a Expert group has no formal status (as it is not explicitly mentioned in EU legislation). Membership of the group is voluntary and decisions by the group or guidelines adopted by the group are not legally binding.

This document describes the terms of reference of the Article 13a Expert Group and formalizes an understanding between the members of the Article 13a Expert Group about sharing of sensitive information.

2 Goal of the group

The goal of the ENISA Article 13a Expert Group is

1. to agree on the necessary technical details to allow for an efficient and effective implementation of Article 13a that is consistent and, as much as possible, harmonized across the EU,
2. to facilitate voluntary exchange of information between experts of National Competent Authorities about security threats, security incidents, lessons learned, standards, good practices and tools,
3. to facilitate review and input on the ENISA papers.
4. to propose activities for the ENISA work program.

In practice, this has resulted, for example, in the development of guidelines on incident reporting, security measures, as well as incident reporting tools and procedures to facilitate the annual summary reporting.

The group does not have a formal work program. Standard topics and activities are:

- Practical and technical details regarding the implementation of security incident[1] notification by providers to National Competent Authorities.
- Informing other Member States and ENISA about incidents with cross-border impact
- Annual summary reporting about notified incidents to ENISA and the Commission
- Information exchange between the Member States about security incidents, vulnerabilities and threats
- Review and validation of ENISA papers related to Article 13a
- Physical meetings
- Guidelines for authorities on the implementation of Article 13a
- Development of procedures and tools to support the implementation of Article 13a.

[1] The term security incident, in this document, means “breaches of security” or “loss of integrity “with an impact on the operation of electronic communications networks and services, as mentioned in Article 13a of the Framework Directive (2009/140/EC).

Members of the group can propose additional activities to the chair. The chair asks the group for a decision before starting the new activity.

3 Members of the group

The ENISA Article 13a Expert Group is an informal group. Members of the group are experts, representatives of their organisations having a specific role and competence in the Article 13a Regulation.

The members can express their views, yet these are not binding for their organisation.

There are two types of members: Full members and associate members.

Full members are experts from national competent authorities in the EU Member States and EFTA countries, with the officially established role of authority in the context of Article 13a, relevant to the goals of this expert group.

Associate members of the group are:

- Experts from ENISA, acting as the secretariat of the group (see below)
- Experts from the European Commission, acting as observers.
- Experts from ministries or national competent authorities, with relevant tasks or competences from EU candidate countries.

The main difference between associate members and full members is that decision making and chairing of the group is restricted to full members (see below).

Members join the group in their professional capacity as employees of their organization. Experts must have been designated by their organization to participate and represent their organization in the expert group.

Experts can join the group by sending an email to Secretariat_Article13EG@enisa.europa.eu. This email should confirm that they have been designated by their organization to join the group.

4 Meetings of the group

Meetings, physical meetings and virtual meetings like teleconferences are open for both full and associate members.

Only members of the group are entitled to participate in the meetings or teleconference. In case a member of the group would like to invite other experts to a meeting, for example from other national authorities, academia, etc, then this needs to be communicated and confirmed with the chair of the group.

Occasionally, the chair may invite relevant experts, from public or private sector, who are not members, for the entire or a part of the meeting, on a case-by-case basis. The chair will communicate such invitation of non-members beforehand.

Agenda and minutes are accessible and shared only with (full and associate) members of the group.

The aim is to hold three physical meetings per year, each time in a different European country, to ensure that over time the travel time and costs are similar for all group members. One of the physical meetings, usually the first one, at the start of the year, has an open session with talks and participants from the telecom sector.

The second meeting focuses on the past incident reporting round and the draft EU wide annual report. This meeting is often used to agree on the direction of work done by the group.

The third meeting is used for finalizing studies and work done by the group, such as guidelines, thresholds for reporting before the new year starts, and to prepare for the next round of reporting.

5 Chair, vice-chair and secretariat of the group

ENISA provides the secretariat of the group. The tasks of the secretariat are:

- Supporting the chair with its tasks
- Supporting the organization of meetings (in terms of logistics and budget)
- Supporting the drafting of meeting agendas
- Supporting the drafting of meeting minutes
- Supporting activities of the group, such as the development of guidelines or tools.
- Supporting analysis of security incidents involving electronic communication services from several Member States upon request of the supervisory body of at least one involved Member State.

ENISA supports the chair with its tasks and ensures there is a smooth functioning of the group. ENISA, also ensures the continuity of the group, by keeping an archive of meeting agendas, meeting minutes, presentations etc. and ensuring a smooth handover between subsequent chairs of the group.

ENISA ensures that the archive is only accessible to members of the group.

The chair and vice chair are full members of the group, i.e. an expert from a supervisory body or national authority of an EU Member State, elected by the group for a period of 2 years.

The tasks of the chair are:

- Setting the date and location of the meetings
- Setting the agendas of meetings
- Chairing and conducting meetings
- Circulating meeting minutes for input and approval
- Consulting the group on the adoption of technical guidelines and procedures for the group, (see Decision making).
- Consulting the group on the initiation of new activities, following proposals by members (see Decision making).
- Both the minutes and agenda are printed using template and letterhead of the organization of the chair, i.e. the relevant supervisory body.

The chair conducts the meetings, in close collaboration with the secretariat, ENISA, and where relevant instructs the secretariat to record decisions or action points, such as the approval of drafts, in the meeting minutes. After each meeting, the chair receives draft minutes from ENISA and circulates them for approval.

The role of the vice chair is to support the chair in their tasks and to replace the chair if needed, for example if the chair cannot join a meeting.

The secretariat is responsible for triggering, in due time, the appointment of a new chair, by circulating a request to the expert group. If there are multiple candidates, the chair will seek a consensus decision by the group.

Together with the election of a chair, the secretariat will also solicit candidates for vice-chair.

6 Working methods of the group

The working language of the group is English. The IT tools of the expert group are:

- ENISA Listserv Mailinglist: Full members and associate members are member of the list. This list is used for communications between members, queries, sharing of non-sensitive information etc.
- ENISA Online working space: The ENISA online working space is an online CMS/portal maintained by ENISA, with an archive of agenda, minutes, drafts, a discussion forum. The online working space is accessible to full members and associate members. The online working space features an issue tracker for sharing information about threats, vulnerabilities with the group. This issue tracker in the online working space can be used for sharing sensitive information with members of the group, by using file attachments.

CIRAS, the reporting tool developed by ENISA, is used by and only accessible to experts from the EU member states and EEA/EFTA partaking in the process of annual summary reporting and cross-border information sharing, as mandated by Article 13a.

Since physical presence in meetings is not always possible draft documents, draft minutes, draft agendas, etc. are always also circulated to all the members of the group. This is done either by directly attaching to an email to the mailing list or when more appropriate (for example when documents are sensitive) by uploading the document in the online workspace and then notifying in the mailing list. See also below in the section “Sharing of sensitive information”.

ENISA will maintain a list of group members, will make it accessible to group members, will ensure that the online portal is only accessible to group members, and will ensure that the mailing list contains only addresses of group members.

7 Decision making by the group

The group is informal and decision making is based on consensus, and used to agree on action points, to agree on minutes, meeting agendas, final guidelines, common procedures, etc.

When there is a disagreement then it is up to the chair to find and reach consensus, for example by proposing a compromise solution that is acceptable to all, even if is not the solution that is preferred by all.

The group can make decisions either by email (for example by explicit approval or by silence procedure), or during meetings, or teleconferences. Note that because some matters are sensitive, some decisions cannot be made via email.

The chair notifies members of the need to make a decision in advance, either by including the decision point in the agenda of a meeting or teleconference, or, in the case of decision by email, by informing the members via email that the group needs to make a decision.

Full members, including the chair may take part in the decision-making (subject to participation in the meeting or teleconference).

Associate members, like experts from ENISA, experts from the Commission, and experts from EU candidate countries, do not partake in the decision making process, but are encouraged to provide feedback and input.

Decisions of the group and action points agreed by the group are documented in the minutes of meetings, and clearly marked as “decisions” or “agreed action points”.

8 Accountability

Members of the group are expected to:

- Partake in the decision making of the group (when full members), or provide input (when associate members)
- Follow the mailing list and read emails sent to the mailing list
- Provide input and comments on drafts
- Respect the principles about sharing of sensitive information (see below)
- Notify the secretariat when they want to leave the group, for example when changing employment.

9 Sharing of sensitive information

One of the goals of the expert group is to facilitate information sharing and sharing of experiences between experts from national competent authorities, in a closed and trusted setting. Unexpected disclosure of information could have negative implications for trust and confidence between the members of the group.

Information shared during meetings, discussions in the mailing list, documents circulated in the mailing list, comments made by experts during meetings, should be handled according to their marking (see Annex A).

To avoid misunderstandings that could damage trust between the members, the expert group has an understanding, i.e. an informal agreement, about the sharing and handling of sensitive information.

The understanding on sharing and handling of sensitive information is explained in detail in the annex of this document. All members of the group, full and associate members, are expected to adhere to this understanding.

10 National laws

Nothing in this document shall cause prejudice to national laws and regulations of the Member States regarding public access to documents, government access to documents, the protection of personal data, the protection of classified information, and so on.

11 Data protection

Personal data of participants will be processed in accordance with EU Regulation 2018/1725.

Annex A: Understanding on sharing of information and handling of sensitive information

This annex explains in more detail the expert group's understanding on sharing of information and handling of sensitive information. Note that, as already mentioned in Section 10, this annex does not cause prejudice to existing national or EU legislation on sharing of information or classifications like EU-CI.

Traffic light protocol labels

The understanding is that members use the traffic light protocol[2] to label information. TLP is an existing protocol that is widely used for sharing sensitive information in collaborative settings. TLP has 4 colours:

- **RED** (do not share)**:** The information can *not* be shared with anyone. For instance, in the context of a meeting, for example, RED information is limited to those present at the meeting. In the context of an email message, RED information is limited to the named recipients of the email.
- **AMBER** (need to know): The information *can* be shared, but only with colleagues inside your organization on a *need-to-know* basis.
- **GREEN** (community): Information may be circulated more widely within a particular relevant community, of subject matter experts for instance. The information cannot be published on the internet or made public.
- **WHITE** (public)**:** Information is public. The information may be distributed or published without restriction, taking into account standard copyright rules, if applicable.

The understanding is that members of the group, before sharing information, include TLP labels clearly typed with capitals, clearly visible, for example on the cover of documents, in the page header, at the start of an email, at the start of a presentation, etc. It is understood that the other members of the group adhere to these TLP labels when they encounter them.

Default label is TLP:AMBER

When no label is present on documents uploaded to the workspace or in information circulated on the mailing lists, the information should be treated as if it is TLP:AMBER.

Communication tools and use of labels

Considering the working methods and communication tools of the group, and taking into account the technical features of these tools in terms of access control, encryption, etc, the understanding is that[3]:

- **TLP:RED** labels should be avoided as much as possible. **TLP:RED** should only be shared face-to-face in physical meetings, explaining clearly that the information is **TLP:RED**.
- **TLP:RED** should *not* be shared in the mailing list nor in emails, *not* be uploaded in the online work space, should *not* be included in meeting minutes nor be registered or documented by experts in their organizations records. If online communication is needed, experts should on a bilateral basis, agree suitable electronic communication means, depending on circumstances and needs, such as Signal or PGP.

[2] The traffic light protocol is an informal originator labelling scheme for the sharing of sensitive information, originally developed by the UK Centre for the Protection of National Infrastructure (CPNI), in order to encourage greater sharing of information and in particular the sharing of information which are sensitive but not classified.

[3] Unlike traditional information classification policies, TLP does not prescribe specific tools or encryption methods

- **TLP:AMBER** information *can* be uploaded in the online work space, and attached as files to issues in the issue tracker, because the online workspace uses encryption and authenticates and restricts access to members of the group only.
- **TLP:AMBER** information *can* be referenced in minutes, while linking to the actual information, which should be stored only in the online work space or issue tracker, because minutes of the meeting are often circulated via emails and in the mailing list.
- **TLP:AMBER** information should *not* be shared in the mailing list, because of weaknesses in the email protocol (such as inconsistent use of transport layer encryption during email exchange between mailservers).
- **TLP:GREEN** information can be shared in emails, mailing lists, uploaded in the online workspace etc. but cannot be re-published online on public websites.