TERMS OF REFERENCE - ENISA ECASEC EXPERT GROUP

1. INTRODUCTION AND BACKGROUND

In 2009, Article 13a was introduced as part of the Telecoms Framework Directive[1]. Article 13a required EU Member States to ensure that providers of electronic communications networks and services take appropriate security measures to protect their security and integrity.

In 2010, European Union Agency for Cybersecurity (ENISA), European Commission (EC), National Ministries and National Competent Authorities for the security of electronic communications initiated a series of meetings (workshops, conference calls) to support a harmonized implementation of Article 13a.

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 Telecoms Framework Directive.

In December 2018, a new set of telecom rules called the European Electronic Communications Code[2] (abbreviated as the EECC) was adopted.

EU countries had to transpose this EU directive into national law by 21 December 2020.

Article 40 of the EECC, which replaces the above-mentioned Article 13a, contains detailed security requirements for electronic communication providers. Article 41 of the EECC, which replaces Article 13b of the Framework Directive, outlines how competent authority can enforce these security requirements. Although the security requirements under the EECC are similar to the security requirements under the Framework directive, there are differences between the two legal acts.

An overview of the main differences can be found in the ENISA paper “Security supervision under the EECC”[3].

To reflect this legislative change the Article 13a group has changed its name to ECASEC: European Competent Authorities for Secure Electronic Communications.

In December 2022, Directive (EU) 2022/2555 was adopted, the NIS 2 Directive[4], repealing the NIS Directive (Directive (EU) 2016/1148)[5] and amending the EECC. Specifically, while Articles 40 and 41 will be removed from the EECC, providers or electronic communications and services will now come under the purview of NIS 2 Directive.

As with Article 13a, ENISA supports the EU Member States with the implementation of Articles 40 and 41 of the EECC and the respective Articles of the NIS 2 directive to ensure there is an effective, efficient, and harmonized approach to information security supervision across the EU.

[1] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (OJ L 337, 18.12.2009, p. 37–69).

[2] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. (europa.eu)

[3] Security Supervision under the EECC — ENISA (europa.eu)

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80–152).

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

The ENISA ECASEC Expert group has no formal status, as it is not explicitly referred to in EU legislation. Membership in the group is voluntary, and decisions and guidelines adopted by it are not legally binding. This document describes the terms of reference of the ECASEC expert group and sets out the rules on sharing of sensitive information within it.

2. GOAL OF THE GROUP

The goal of the ENISA **ECASEC** expert group is**:**

- to agree on the technical and organisational measures for an efficient and effective implementation of the relevant provisions of Articles 40 and 41 of the EECC and, as of October 2024, of the provisions of the NIS 2 directive that pertain to telecom security, incident reporting and supervision of electronic communications providers,
- to facilitate voluntary exchange of information between experts of National Competent Authorities, including on security threats, security incidents, lessons learned, standards, good practices and tools,
- to facilitate review and provide input on ENISA papers,
- to propose activities for ENISA work program.

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

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

- Practical and technical details regarding the implementation of security incident notification by electronic communication providers to National Competent Authorities.
- Informing the group members about incidents with cross-border impact
- Annual summary reporting about notified incidents to ENISA and the Commission
- Information exchange between the group members about security incidents, vulnerabilities and threats
- Review and validation of ENISA papers related to technical topics of telecom security and also guidelines, procedures and tools to support the implementation of relevant legislative provisions (e.g. EECC, NIS 2 Directive, etc)
- 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

Members of the group are experts, representatives of their organisations having a specific role and competence in telecom security. 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.

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.

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 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).

4. MEETINGS OF THE GROUP

Meetings are open to both full and associate members.

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

Occasionally, the chair may invite relevant non-member experts from public or private sector for the entire or part of a meeting. The chair will communicate to the group such invitation of non-members beforehand.

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

The group aims to meet three times per year.

The aim is to hold at least two physical or hybrid meetings per year, each time in a different country, to ensure that over time the travel time and costs are similar for all group members.

Whenever technically feasible, meetings are recorded to facilitate generation of the minutes.

5. CHAIR, VICE CHAIR(S) AND SECRETARIAT OF THE GROUP

The chair and vice chair(s) are full members of the group, 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)

The chair conducts the meetings, in close collaboration with the secretariat, ENISA, and where relevant instruct 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(s) 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 and vice chair(s) by circulating a request to the expert group. If there are multiple candidates, the chair will seek a consensus decision by the group.

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

- Supporting the chair/vice chair(s) with their 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 more than one country – member of the group upon request of a supervisory body of at least one of the countries involved.

ENISA also ensures continuity of the group by keeping an archive of meeting agendas, meeting minutes, presentations and other relevant documents, and ensuring a smooth handover between subsequent chairs of the group.

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

6. WORKING METHODS OF THE GROUP

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

- ENISA Listserv Mailing list: Used for non-sensitive communications by members of the group
- ENISA Online working space: ENISA online working space is an online CMS/portal maintained by ENISA, including an archive of documents such as agendas, minutes, drafts and papers. The online working space is accessible to members.
- ENISA CIRAS (Cybersecurity Incident Reporting and Analysis System) tool, the incident reporting tool developed, administered and maintained by ENISA. It is accessible by experts from EU member states and EEA/EFTA countries participating in the process of annual summary reporting and cross-border information sharing.
  CIRAS also includes a discussion forum for sharing information about supervision topics, incidents, threats and vulnerabilities with the group.

7. DECISION MAKING BY THE GROUP

Decision making is based on consensus, and used to agree on matters such as action points, minutes, meeting agendas, final guidelines or common procedures.

In cases of a disagreement, the chair will take best effort to reach a 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 a silence procedure), or during meetings. Since some matters are sensitive, some decisions cannot be made by email.

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

In case of real-time voting in a meeting, full members, including the chair, may take part in the decision-making, if they are present in the meeting.

Associate members, such as 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 clearly marked as “decisions” or “agreed action points”.

8. ACCOUNTABILITY

Members of the group are expected to:

- Participate in the decision making of the group (when full members), or provide input (when associate members)
- Follow the mailing list
- Provide input and comments on draft documents
- Respect the principles of sharing 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 between experts from national competent authorities in a closed and trusted setting. Unwanted disclosure of sensitive information could have negative implications for trust and confidence between the members of the group.

Any information exchanged by the group, including that 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).

The rules on sharing and handling of sensitive information are set out in the Annex to this document. All members of the group are expected to adhere to them.

10. NATIONAL LAWS

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

11. DATA PROTECTION

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

ANNEX A: RULES 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. Please 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, such as EU-CI.

Traffic light protocol labels

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 cannot be shared with anyone. For instance, in the context of a meeting, 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 ECASEC and the member's authority 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.
- **CLEAR (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

Notwithstanding the rules set out below, 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 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:

- **TLP:RED** 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, bilateral emails, be uploaded in the online work space, be included in meeting minutes nor be registered or documented by experts in internal documents in the authorities. 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.
- **TLP:AMBER** information can be uploaded in the online work space, and attached as files to issues in the CIRAS tool, 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.
- 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.