European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

EXECUTIVE DIRECTOR DECISION

ED DECISION No 143/2020

OF THE EXECUTIVE DIRECTOR OF THE AGENCY

of 16 November 2020,

on THE NATIONAL LIAISON OFFICERS NETWORK

(hereinafter referred to as "the NLO Network" or "the Network"),

THE EXECUTIVE DIRECTOR OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Having regard to

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (hereinafter referred to as "Cybersecurity Act"), and in particular Article 23 thereof;
- Decision No MB/2020/04 of the Management Board of the European Union Agency for Cybersecurity, hereinafter referred to as "ENISA" or "the Agency", on Setting up a National Liaison Officers Network;

Whereas

(1) The establishment of the NLO Network should enable ENISA to maintain regular dialogue with the EU Member States and National Liaison Officers, hereinafter referred to as "NLOs", shall act as a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme.

(2) The NLO Network was initially set up in 2004 as an informal point of reference into the Member States. As of 27 June 2019 the NLO Network has become a statutory body of ENISA.

(3) The NLO Network should not duplicate the work of the ENISA Management Board nor of other EU fora (e.g. the Cooperation Group, the EU Council preparatory bodies and others).

(4) The NLO Network and NLOs should focus on the implementation of ENISA's activities as provided in its annual work programme to the benefit of ENISA and the Member States.

(5) The NLO Network working arrangements, including the tools to communicate and exchange information, should be decided by the NLO Network in consultation with the Agency.

(6) The NLO Network has decided on rules of procedure in consultation with the Agency.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION

Article 1
Composition of the NLO Network

1. In accordance with Article 23 (1) of the Cybersecurity Act and Article 2 (1) of Decision No MB/2020/04 of the Management Board of ENISA on Setting up a NLO Network, the Management Board of ENISA, acting on a proposal from the Executive Director, shall set up a NLO Network composed of representatives of all Member States. Each Member State shall appoint one representative to the NLO Network.
2. In accordance with Article 2 (2) of Decision No MB/2020/04 of the Management Board of ENISA on Setting up a NLO Network, representatives designated by the European Commission can participate in the NLO Network as observers.

Article 2
Role of the Network

The role of the Network is laid down in Article 23 of the Cybersecurity Act and Article 1 of Decision No MB/2020/04 of the Management Board of ENISA on Setting up a NLO Network. The NLOs, in accordance with Article 23 (3) of the Cybersecurity Act, shall act as a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme. As a consequence, the single programming document of ENISA shall serve as a main reference point for the NLO Network and its activities. The Network shall receive the single programming document no later than 10 calendar days following its adoption in the ENISA Management Board in each year. The final version after definitive adoption of the general budget of the Union and any subsequently amended versions shall be made available to the NLO Network by the NLO secretariat.

Article 3
NLO secretariat

The Agency shall be responsible for providing the secretariat for the NLO Network.

Article 4
Documentation to be sent to members of the NLO Network

1. The NLO secretariat shall send the invitation to meetings and the draft agenda to the Network members well in advance of the meeting and no later than fourteen calendar days before the date of the meeting.

2. The secretariat shall send documents on which the Network is being consulted to the Network members by email and/or upload them on a dedicated website no later than fourteen calendar days before the date of the meeting.

3. In urgent or exceptional cases, the time limits for sending the documentation mentioned in paragraph 1 and 2 may be reduced to five calendar days before the date of the meeting.

Article 5
Correspondence

Correspondence to Network members shall be sent to the email address, which they provide for that purpose.

Article 6
Written procedure

1. If necessary, the Network's opinion on a specific question may be delivered via a written procedure. To this end, the NLO secretariat sends the Network members the document(s) on which the Network is being consulted under the conditions of Article 4.

2. However, if a minimum of six Network members asks for the question to be examined at a meeting of the Network, the written procedure shall be terminated without result and the secretariat shall convene a meeting of the Network as soon as possible.

3. The secretariat shall inform the members of the Network of the outcome of a written procedure in due time.

4. Consultations among Network members in the form of a written procedure on specific issues shall be possible based on a preceding call for volunteers among the Network members.

Article 7
Convening of meetings and meeting agenda

1. Rules for the convening of meetings are laid down in Article 3 of Decision No MB/2020/04 of the Management Board of ENISA on Setting up a NLO Network.

2. Rules applicable to reimbursements of travel and subsistence expenses incurred by the NLO Network members in connection with meetings relating to NLO Network activities are laid down in Article 4 of Decision No MB/2020/04 of the Management Board of ENISA on Setting up a NLO Network.

3. A provisional agenda shall be drawn up by the NLO secretariat and sent to the Network under conditions laid down in Article 4 (1). NLOs shall have the right to request inclusion of specific agenda items no later than two working days before the date of the meeting.

4. In accordance with Article 23 (1) of the Cybersecurity Act, meetings of the NLO Network may be held in different expert formations. The NLO secretariat shall inform the NLOs under conditions of Article 4 (1) that a meeting or part of a meeting may be held in a specified expert formation and provide the reasoning for the expert formation. The NLO secretariat shall ask the NLOs for suitable national experts to participate in such cases. NLOs shall have the right to attend meetings in expert formation.

Article 8
Meeting minutes

1. Summary minutes on the discussion on each point of the agenda shall be drafted by the NLO secretariat. The secretariat shall send the draft minutes to the Network members no later than one month after the meeting.

2. The summary shall not mention the individual position of the members during the Network's deliberations, unless a member asks for its position to be recorded in the minutes.

3. The members of the Network shall send any comments they may have on the minutes to the NLO secretariat in writing. If there is any disagreement, the matter shall be discussed by the Network. If the disagreement persists, the relevant comments shall be annexed to the final summary.

Article 9
Attendance list

At each meeting, the secretariat shall draw up an attendance list specifying, where appropriate, the authorities, organisations or bodies to which the participants belong.

Article 10
NLO Network Portal

1. The Group shall have a dedicated, non-public, web portal run by the secretariat where the agenda and documents of meetings will be uploaded.

2. Other documents and information shall be included in the portal as decided by the NLO Network in consultation with the Agency.

Article 11
Voting procedures

1. The Network works on the basis of consensus. Voting shall only be necessary when consensus on a specific issue is not achieved. Members of the Network, the NLO secretariat and the Chair shall indicate a non-consensus situation on a specific issue. In case of non-consensus the Chair shall decide to continue to the voting procedure or continue discussions aiming at consensus-building.

2. For proposals submitted for voting to the Network or requested by a simple majority of its members, the Network, consisting of one appointed NLO per Member State as laid down in Article 23 (1) of the Cybersecurity Act, shall adopt its decisions by simple majority of its appointed members.

3. Observers shall not have the right to vote.

4. Each member has one vote. In addition to his/her own vote, each voting member may cast one vote that he/she has received by proxy in case of absence of another member, which has to be notified to the secretariat.

5. Unless a secret ballot is requested by at least one-third of the voting members, votes shall be taken by show of hands.

6. For each and every decision adopted by a vote, the result, along with the numbers of votes cast, shall be recorded.

7. Each member shall have the right to ask to have its position recorded in the minutes on specific issues.

Article 12
NLO alternates and change of NLO

1. In case of short-term absence, sickness or other reasons, which do not require the nomination of a new NLO, NLOs shall be able to indicate an alternate for a specified time period to the NLO secretariat.

2. In case of change of post, retirement or other reasons, which require the nomination of a new NLO, the applicable Member State nominates one new NLO in accordance with national procedures for such nominations.

Article 13
Third countries

The participation of representatives of third countries, having concluded agreements with the European Union for the participation in ENISA, may take place in accordance with the working agreements referred to in Article 42 (2) of the Cybersecurity Act.

Article 14
Cooperation with Management Board representatives

In accordance with Article 23 (4) of the Cybersecurity Act, NLOs shall cooperate closely with the Management Board representatives of their respective Member States. The Network shall not duplicate the work of the Management Board or of other Union forums.

Article 15
Conflict of Interest

1. The following obligation shall also apply to the members of the NLO Network. Article 25 of the Cybersecurity Act provides for the obligation for the members of the Management Board, the Executive Director and officials seconded by Member States on a temporary basis to make a declaration of commitments and a declaration indicating the absence of any direct or indirect interest, which might be considered prejudicial to their independence. Such declarations shall be made in writing and shall be updated regularly, preferably on a yearly basis.

2. Therefore, as a rule, any person facing a conflict of interest situation is under a duty of informing and, as appropriate, discussing the best way of avoiding that the situation has an impact on the validity of the decisions.

3. There is a conflict of interests where the impartiality and objectivity of a decision, opinion or recommendation of the Agency, including its bodies, is or might in the public perception be compromised by an interest held by, or entrusted to, an individual working for the Agency.

4. A conflict of interest exists when a person appointed to a function has a personal or vested interest in the outcome of decisions resulting from that function. Consequently, a person must not be involved in any decision during the course of his/her duties with the knowledge that there is an opportunity to further his/her personal interests.

5. A conflicting interest could be defined as any situation where anyone acting on behalf of ENISA, involved in the conduct of a procedure where that person may influence the outcome of that procedure, has, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise his or her impartiality and independence in the context of the procedure.

6. It must be highlighted that an "interest" declared is not automatically considered as a conflict of interest. Therefore, the immediate aim of a conflict of interest policy is to protect the integrity of official policy and administrative decisions and of public management generally.

7. Each case should be decided ad hoc.

Article 16
Other provisions

1. Annex I includes good practices that are advised to be followed by the members of the NLO Network.

2. This decision shall enter into force on the date of its signature.

Done in Athens, 16 December 2020

Juhan Lepassaar

Executive Director

ANNEX I

GOOD PRACTICES

The following recommendations shall serve NLOs as a reference for good practices in their function.

1. Community building:
   - NLOs manage, develop or use already existing contact or mailing lists of relevant cybersecurity experts and stakeholders in their Member State. NLOs can further leverage social media for the purpose of community building (e.g. LinkedIn, Twitter).

2. Dissemination/information:
   - ENISA keeps NLOs informed about its activities by means of targeted communication channels in order to further disseminate ENISA activities within the NLO managed community in the Member State.
   - NLOs shall – and are encouraged to – keep ENISA and the NLO Network informed about events with a cybersecurity relevance in their Member States.
   - NLOs overview cybersecurity developments in their Member State and submit national news for possible publication on the ENISA website ("News from the Members States" section).
   - ENISA seeks to set up a private portal for information sharing with NLOs. This portal shall become the main database for ENISA NLO cooperation and coordination. Following the setting up of a portal, ENISA will consider additional measures to increase contact and engagement between NLOs in the interest of an improved information flow on roles and good practices.

3. Feedback:
   - NLOs may collect feedback from their national communities on ENISA activities. This suggests that NLOs could both retrieve information on ENISA related topics and activities in their national communities, e.g. utilisation of deliverables produced by current (or past) work programmes, and request information from ENISA triggered by the needs in their country.
   - NLOs may collect ideas and requirements about ongoing cybersecurity issues in the interest of the Member State, an industry sector or a public service etc.
   - ENISA may collect NLO feedback for further consideration and information of the ENISA Management Board, the ENISA Executive Board, the ENISA Advisory Group and the Executive Director.
   - Feedback mechanisms shall be subject to discussion and specification within the Network.