

# CALL FOR APPLICATIONS: ENISA'S AD-HOC WORKING GROUP ON THE EU CYBERSECURITY MARKET

## 1. INTRODUCTION

The Ad-Hoc Working Group on EU Cybersecurity Market will aim at supporting the European Union Agency for Cybersecurity (ENISA) to perform analyses and monitoring of the cybersecurity market as foreseen under the Cybersecurity Act<sup>1</sup>. In addition, the group will contribute to ENISA's preparatory and supporting activities, as foreseen under the Cyber Resilience Act<sup>2</sup>.

Cybersecurity market analysis and monitoring helps understand the level of uptake of cybersecurity related products, services and processes in the relevant market and contribute to achieve a high common level of cybersecurity. Information on the demand and the supply of cybersecurity will be the driver for the deployment of a variety of measures to vitalise the internal cybersecurity market, take proper market deployment measures, promote innovation and close market gaps.

## 2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881, Art. 20 (4), the Executive Director of the EU Agency for Cybersecurity may set up ad hoc working groups (AHWGs) composed of experts, whenever necessary and within ENISA's objectives and tasks. AHWGs provide ENISA with specific advice and expertise. Prior to setting up an AHWG, the Executive Director of ENISA shall inform the Agency's Management Board.

The members of the AHWGs are selected according to the highest standards of expertise, aiming to ensure appropriate balance according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry, users, and academic experts in network and information security<sup>3</sup>.

<sup>1</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881> (accessed 22/05/2025). See in particular Art. 8 Par 7.

<sup>2</sup> Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed 22/05/2025). See in particular, Art. 60.

<sup>3</sup> Recital 59 of the Regulation (EU) 2019/881.

As stipulated in the CSA<sup>4</sup>, ENISA should *'perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union'*<sup>5</sup> (Art. 8 Par. 7 CSA).

ENISA plays also a role under the CRA<sup>6</sup> in terms of market analysis and preparation of market sweeps (in other words simultaneous coordinated control actions) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to the CRA. More concretely, ENISA should submit to the market surveillance authorities' proposals for categories of products with digital elements for which sweeps could be organised. ENISA should do so based, inter alia, on the notifications of vulnerabilities and incidents it receives. In particular, sweeps should be conducted *'where market trends, consumer complaints or other indications suggest that certain categories of products with digital elements are often found to present cybersecurity risks'*<sup>7</sup>

Moreover, in its role under the CRA, *'ENISA should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with [...CRA] of products with digital elements across several Member States or identify categories of products for which sweeps should be organised. In exceptional circumstances, ENISA should be able, at the request of the Commission, to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the proper functioning of the internal market'*<sup>8</sup>.

To further cover the EU cybersecurity market as foreseen in the CSA and to support ENISA in its tasks foreseen in the CRA, ENISA seeks the involvement and support of public and private experts to contribute to the comprehensive coverage of ENISA outputs by providing suitable advice and expertise concerning important aspects thereof. Main purpose of this AHWG is to provide this support to ENISA.

This AHWG contributes in particular to Activity 8 *Supporting European cybersecurity market, research & development* of the ENISA Single Programming Document 2025-2027<sup>9</sup>, which *'seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular for SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market'*.

The Management Board has been informed by the Executive Director of ENISA of the intention of setting up this AHWG on 29 September 2025 and consequently, ENISA is launching this Call for expression of interest.

<sup>4</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881> (accessed 22/05/2025).

<sup>5</sup> See also Recital 42 CSA.

<sup>6</sup> Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed 22/05/2025).

<sup>7</sup> Recital 114. See also Art. 60 on Sweeps.

<sup>8</sup> Recital 115 CRA. See also Art. 60 on Sweeps.

<sup>9</sup> ENISA Single Programming Document 2025-2027, [https://enisa.europa.eu/sites/default/files/2025-02/17\\_02\\_2025\\_ENISA%20Single%20Programming%20Document%202025-2027.pdf](https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf) (accessed 22/05/2025).

### 3. SCOPE OF THE AD HOC WORKING GROUP

In line with the CSA<sup>10</sup>, ENISA is tasked to *'perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union'* (Art. 8 Par. 7 CSA)<sup>11</sup>. In addition ENISA's is expected to conduct preparatory and supporting activities under the CRA<sup>12</sup>. The Ad-Hoc Working Group on EU Cybersecurity Market, to be established via this Call, will support ENISA to perform these activities under the CSA and the CRA.

#### Example of activities that the members of this group might undertake:

- 1) Assist ENISA in the implementation, dissemination, and taking up of its work in the area of cybersecurity market analysis and cyber resilience (e.g., data collection, reports, guidelines, technical advice, and event preparation);
- 2) Help ENISA identify significant market segments, products and services, to focus on its cybersecurity market analyses and monitoring;
- 3) Provide ENISA with guidance on how to analyse and monitor the cybersecurity market, including helping ENISA maintain and improve the ENISA Cybersecurity Market Analysis Framework (ECSMAF)<sup>13</sup> and promote its usage by the Member States and other stakeholders;
- 4) Support ENISA in creating and maintaining a cybersecurity market analysis community and identify capacity building activities to foster the sustainable growth of a cybersecurity market analysis and monitoring capacity at EU and national level;
- 5) Support ENISA in facilitating the collection and the sharing of good practices, analysis and monitoring initiatives, frameworks, taxonomies, data and data sources, etc. in the area of cyber security market;
- 6) Help ENISA identify synergies between its work in the area of cybersecurity market and other initiative in this area;
- 7) Support ENISA toward CRA-related tasks, such as establishing a methodological framework for the identification of categories of products with digital elements to propose for market sweeps and the preparation of market analysis to support ENISA's role vis-a-vis market surveillance authorities;
- 8) Help ENISA in other tasks the Agency might be asked to perform to assist the Member States or EUIBAs in the area of market analysis and cyber resilience.
- 9) Support ENISA in the coordination of the work with other relevant expert groups, networks and stakeholders;
- 10) Provide input and recommendations to and review documentation related to ENISA work, both in the area of cybersecurity market analysis and monitoring and in cyber resilience.

The tasks of the AHWG will be complementary to and coordinated with the tasks of:

- the Expert Group on Cybersecurity of Products with Digital Elements<sup>14</sup> established by the European Commission's Directorate-General for Communications Networks, Content and Technology ('DG CONNECT');

<sup>10</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881> (accessed 22/05/2025).

<sup>11</sup> See also Recital 42 CSA.

<sup>12</sup> See in particular Art. 60, Recitals 117 and 115.

<sup>13</sup> ENISA Cybersecurity Market Analysis Framework (ECSMAF) - V2.0, <https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0> (accessed 23/05/2025).

<sup>14</sup> <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967> (accessed 20/11/2024).

- relevant work and activities performed by European Cybersecurity Competence Centre (ECCC) and by the National Coordination Centres (NCCs);
- the dedicated administrative cooperation group (ADCO) for the cyber resilience of products with digital elements to be established under the CRA;
- groups established under the CSA, such as the European Cybersecurity Certification Group (ECCG), the Stakeholder Cybersecurity Certification Group (SCCG), the NIS Cooperation Group, the CSIRTs network and other ENISA AHWGs.

This AHWG will co-operate with:

- the European Commission Expert Group on Cybersecurity of Products with Digital Elements;
- the CRA ADCO (when established);
- other groups relevant/complementary to its tasks (see list above).

The preliminary estimate of the duration of this AHWG is for up to **three calendar years** from the issue of the respective Agency Decision that signals the kick-off date of this working group's operation; extension of the mandate of this working group is possible, should the scope of the work be not completed in the foreseen timeframe.

The members of the AHWG (including those in the reserve list) may be requested by the Agency for further or specific engagement upon remuneration and based on the point 8.2 of this Call.

## 4. COMPOSITION AND APPOINTMENT OF MEMBERS AND OBSERVERS

**Composition:** 'The working group shall be composed of a Chairperson, who is designated from ENISA staff by the Executive Director, and members of the AHWG. When and where necessary, the Executive Director may also designate Vice-Chairperson(s) from ENISA staff. The AHWG will be composed of up to 20 selected members-leading experts, based on the requirements of this open Call'<sup>15</sup>.

For a balanced composition of the AHWG, ENISA will take into account factors such as: relevance and public visibility of profile to carry-out the afore-mentioned activities, sector, geographical and gender balance among selected members to cover various stakeholder groups both from the cybersecurity and communications field in the public, private, academia, and civil society organisations.

**Reserve list:** Besides members of the AHWG, ENISA is likely to appoint a reserve list, in accordance with the same conditions that apply to members. While indeed an initial cohort of up to 20 members will be appointed to the AHWG, ENISA reserves the right to draw from the reserve list at any time should additional expertise be required to support the group's mandate.

Moreover, reserve list members may be called upon under the same terms and conditions as appointed members, also to replace any members who are absent or otherwise indisposed. In case of a member's unavailability, disqualification or resignation, the Chairperson of the AHWG can appoint a member (or

<sup>15</sup> Art. 4 of the Decision No MB/2022/5 of the Management Board of The European Union Agency For Cybersecurity (ENISA) on the Establishment and Operation of Ad Hoc Working Groups and Repealing MB Decisions No MB/2013/11 and No MB/2019/11, [https://www.enisa.europa.eu/sites/default/files/all\\_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf](https://www.enisa.europa.eu/sites/default/files/all_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf) (accessed on 30 July 2025).

members) from the reserve list, to replace any members who are indisposed. The new member(s) will be appointed for the remaining of the term of the AHWG.

Members who are no longer capable to contribute effectively to the group's deliberations, who in the opinion of ENISA do not comply with the conditions set out in Article 339 of the Treaty on the functioning of the European Union or who resign, shall no longer be invited to participate in any meetings of the AHWG and may be replaced for the remaining duration of the AHWG.

**Appointment:** Members of the AHWG will be appointed *ad personam* by the Executive Director of ENISA from a list of suitable experts selected through this open Call. Appointed members shall serve in their personal capacity, acting independently and in the public interest, without directly representing any organisation or stakeholder group.

**Observers:** Permanent observers may include a range of organisations with public-interest missions, such as national regulatory bodies, sectoral and consumer associations, academic consortia, and other stakeholders serving a broader public goal. These entities may apply for observer status as described in the section 9 (Application procedure) of this Call, and are required to submit their expression of interest in accordance with Section 9.2 of this Call.

Moreover, as foreseen in the ENISA Management Board Decision No MB/2022/5, 'At the request of the Chairperson, the representatives of the European Commission shall be entitled to be present at the meetings and the National Liaison Officers may take part or nominate representatives to participate as observers'<sup>16</sup>.

## 5. ORGANISATION OF THE AD HOC WORKING GROUP

The Secretariat of the AHWG will be also provided by ENISA to the AHWG. The governance of the group and roles will be decided in collaboration with the selected members as part of the establishment process. ENISA will propose to the AHWG a set of draft rules of procedure to be adopted as appropriate.

The Chairperson convenes the meetings of the working group, administers the agenda of the meeting, ensures a timely distribution of information and documents to all working group members and will address all organisational aspects to facilitate the smooth functioning of the working group. The agenda of the meeting will be provided ultimately 4 working days before the start of the meeting.

The AHWG may be divided into Thematic Groups based upon the different areas of work that will be developed along the project phases. If during the development of the work of the AHWG Thematic Groups are deemed necessary, AHWG members will be invited to participate in the Thematic Groups on the basis of their interest and expertise.

In principle, the AHWG shall convene online, in ENISA premises or as otherwise decided on a proposal of the Chairperson. The bulk of the work would be carried out remotely; conference calls or video conferencing are permitted and encouraged for exchanges between members.

<sup>16</sup> Decision No MB/2022/5 of the Management Board of The European Union Agency For Cybersecurity (ENISA) on the Establishment and Operation of Ad Hoc Working Groups and Repealing MB Decisions No MB/2013/11 and No MB/2019/11, [https://www.enisa.europa.eu/sites/default/files/all\\_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf](https://www.enisa.europa.eu/sites/default/files/all_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf) (accessed on 30 July 2025). See in particular Art. 4.

Support and planning as well as secretariat service will be provided by ENISA, as appropriate. More specifically, ENISA will be responsible for the organisation of the work and support of the working group.

ENISA shall ensure interaction and/ or consultation with the other ENISA advisory bodies, and/ or other stakeholders throughout the lifespan of the AHWG, as appropriate.

ENISA will organise plenaries of the full AHWG with a minimum of **two (2)** meetings per calendar year. There might be more frequent meetings of the different Thematic Groups established to support dedicated work streams.

## 6. CONFIDENTIALITY AND DECLARATIONS OF INTEREST

The members of the AHWG, as well as invited experts and observers, are subject to the obligation of professional confidentiality according to Article 27 of Regulation (EU) 2019/881. More specifically, members of the AHWG shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased. Each member shall sign a confidentiality statement for the duration of the activity.

The AHWG members and observers are also subject to the conditions of Regulation (EC) No 1049/2001 on access to documents<sup>17</sup>.

When members and observers of the AHWG are invited to bring forward their views on aspects or topics related to the work of the AHWG, they may need to be able to consult with their organisations or parties related to them outside their organisation to the extent necessary. They likewise need to be able to share information within their organisation or other relevant parties on a need-to-know-basis, unless the information is indicated in writing, or by announcement of the (Vice)-Chairperson as confidential. Information produced by the AHWG can only be made public upon prior approval of the Chairperson.

After ENISA has published the list of appointed AHWG members and observers, the AHWG members and observers may disclose their membership/status on observers in this AHWG to the public and describe the general scope of the work of the AHWG.

In addition, the members of the AHWG are subject to the obligations of Article 25(2) of Regulation (EU) 2019/881 related to declaration of interests.

---

<sup>17</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Available online at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049> (accessed on 11 August 2025)

## 7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725<sup>18</sup>. For further information, please refer to the data protection notice that is available as a separate document with the Call.

## 8. REIMBURSEMENT OF MEMBERS

### 8.1 REIMBURSEMENT OF THE AHWG MEMBERS FOR THEIR TRAVEL AND SUBSISTENCE EXPENSES IN CONNECTION WITH THE ACTIVITIES OF THE AHWG

The members of the AHWG may be reimbursed for their travel and subsistence expenses in connection with the activities of the working group. If a member comes from a location different than the location required for the provision of services, or the place of the meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost- effective) from the city in which the member is officially registered to the location required for the provision of services, or the place of the meeting.<sup>19</sup>
2. A “daily subsistence allowance (DSA)” applicable to the country in which the meeting will take place. This allowance is set by the European Commission<sup>20</sup> and it covers all daily living expenses including hotel, meals, local travel etc.
3. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible to apply.

Participants who serve as observers may participate in the activities of the AHWG, but are not considered appointed members of the AHWG. Accordingly, in principle they are not eligible for reimbursement of expenses under the provisions outlined in Section 8 of this call. However, ‘Members designated by Member States and industry associations’ representatives may be reimbursed upon submitting a request to ENISA. Participants who require financial support to attend a meeting can make a request to ENISA to be reimbursed according to the ENISA reimbursement rules<sup>21</sup>.

### 8.2 REIMBURSEMENT OF THE AHWG MEMBERS FOR ADDITIONAL TASKS

Members of the AHWG and of the AHWG reserve list that are citizens or permanent residents of the EU or EEA may be engaged in additional tasks conducted within or outside the scope of AHWG activities. In such case, the members of the AHWG (and of the reserve list) shall be eligible for reimbursement under the same rules and procedures as those applicable for the ENISA CEI list of experts<sup>22</sup>. The

<sup>18</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available online at: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj> (accessed on 11 August 2025).

<sup>19</sup> Each invitee, to be eligible for the reimbursement, needs to have their Legal entity and Financial Identification validated on the European Commission's central data base, available under following link: [Forms for contracts - European Commission](https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf).

<sup>20</sup> The latest rates are available to download from: [https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75\\_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf](https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf).

<sup>21</sup> Art. 6 of the Decision No MB/2022/5 of the Management Board of The European Union Agency For Cybersecurity (ENISA) on the Establishment and Operation of Ad Hoc Working Groups and Repealing MB Decisions No MB/2013/11 and No MB/2019/11, [https://www.enisa.europa.eu/sites/default/files/all\\_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf](https://www.enisa.europa.eu/sites/default/files/all_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf) (accessed on 31 July 2025).

<sup>22</sup> [CEI List of Individual External Experts to Assist ENISA | ENISA](#)



remuneration shall be based on the thresholds defined under Article 242 of the Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (Financial Regulation)<sup>23</sup> and under the following rules:

- The remuneration of the experts engaged from the list of the AHWG members shall be based on days of engagement and with a fixed daily fee of 450 euro<sup>24</sup>.
- The annual remuneration of a single expert shall in principle not exceed 30.000 euro.
- The maximum amount of fees that can be paid to a single expert shall be 90 000 EUR during a period of four consecutive calendar years.

AHWG members engaged by ENISA as remunerated experts may also be entitled to the reimbursement of expenses incurred in the course of journeys if invited to meetings organised by ENISA. In such case, the provisions of Article 8.1 shall apply.

**If the applicants for the AHWG wish to be considered for additional remunerated tasks, they will be asked once the selection procedure is completed, to indicate it accordingly and to provide additional documents, namely proof of EU/EEA citizenship or permanent residence and proof of having a bank account in the EU Member State or EEA. They will also need to provide a declaration on their honour, in accordance with the template in Annex 1 to the present Call for expression of interest, duly signed and dated, stating that they are not in one of situations of exclusion as per criteria set out in the Article 138 of the Financial Regulation.**

The validity period of the list of AHWG members (and reserve list) that may be considered for additional remunerated tasks shall follow the validity of the established AHWG.

### 8.3 TRANSPARENCY: EX-POST INFORMATION

If an expert has concluded a contract of more than 15.000 EUR, the name, the locality (region of origin), amount and subject of the contract shall be published on the website of the contracting authority no later than 30 June of the year following the contract award. The information shall be removed two years after the year of the contract award.

## 9. APPLICATION PROCEDURE

### 9.1 CONDITIONS FOR MEMEBRS

Individuals interested in becoming members of this AHWG are invited to submit their application to ENISA using the application form via the EU survey tool<sup>25</sup>, available in the dedicated section on the ENISA website. An application will be deemed admissible only if it is submitted by the deadline.

The list of appointed members and permanent representatives will be made public in the ENISA website.

<sup>23</sup> [Regulation - EU, Euratom - 2024/2509 - EN - EUR-Lex.](#)

<sup>24</sup> This is the maximum amount indicated in the Commission Decision establishing horizontal rules on the creation and operation of Commission expert groups C (2016) 3301 final.

<sup>25</sup> <https://ec.europa.eu/eusurvey/runner/AHWGMKTcall2025>



## 9.2 CONDITIONS FOR OBSERVERS

Public entities and organisations that represent a common interest and generally serve a public goal may apply to participate in the AHWG as permanent observers. These entities should submit an expression of interest addressed to the Executive Director of ENISA clearly outlining:

- Their motivation for participating in the AHWG;
- The public interest or mandate they serve;
- The name and contact details of the proposed permanent observer.

All categories of observers must submit their expression of interest by replying to this call. Exceptionally, they can send their expression of interest - addressed to the Executive Director of ENISA - to [market@enisa.europa.eu](mailto:market@enisa.europa.eu).

Following review, the Executive Director may accept the participation of such organisations and their nominated representative as a permanent observer to the AHWG.

It must be noted that certain categories of observers may participate in the activities of the AHWG also without undergoing a formal selection procedure, but following the nomination. These include:

- Representatives of EUIBAs;
- Public authorities of Member States and EEA/EFTA countries;
- International organisations with a mandate relevant to the scope of this AHWG.

These categories may designate their representatives to the AHWG directly to the Chairperson.

Moreover, as foreseen in the ENISA Management Board Decision No MB/2022/5, 'At the request of the Chairperson, the representatives of the European Commission shall be entitled to be present at the meetings and the National Liaison Officers may take part or nominate representatives to participate as observers' <sup>26</sup>.

## 9.3 DEADLINE FOR APPLICATION

The duly completed applications must be submitted **by 23 October 2025 at 23.59 EET**. The date and time of submission will be established on the European Commission's EU Survey tool, used to collect all submitted applications, upon submission of an application.

This deadline does not apply to the specific categories of observers mentioned above (i.e. representatives of EU EUIBAs, public authorities of Member States and EEA/EFTA countries, international organisations with a relevant mandate), which may participate as observers without a formal application. These entities shall inform the Chairperson of their designated representatives and promptly communicate any changes to ensure the accuracy of representation over time.

<sup>26</sup> Decision No MB/2022/5 of the Management Board of The European Union Agency For Cybersecurity (ENISA) on the Establishment and Operation of Ad Hoc Working Groups and Repealing MB Decisions No MB/2013/11 and No MB/2019/11, [https://www.enisa.europa.eu/sites/default/files/all\\_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf](https://www.enisa.europa.eu/sites/default/files/all_files/MB%20Decision%202022-05%20on%20ad%20hoc%20working%20groups.pdf) (accessed on 11 August 2025). See Art. 4 par. 3.

## 10. TERMINATION OF THE MANDATE OF THE AD HOC WORKING GROUP AND DISSOLUTION

At the moment the tasks of the AHWG are completed, the end-of-life phase of the AHWG will follow. ENISA reserves the right to terminate the AHWG at any moment if there is not anymore, a need for such AHWG.

## 11. ELIGIBILITY CRITERIA

Based on the self-declared application forms received, only candidates who meet the following minimum criteria will automatically be considered to be included in the list of external experts dependent on endorsement by an evaluation committee:

- Have fully completed their application form;
- Are a national of, or working for a legal entity of one of the Member States of the EU or EEA; *(Nationals outside EU/EEA are also eligible to apply for the membership to the AHWG but they cannot be remunerated for certain tasks under the AHWG as per paragraph 8.2.);*
- Have a bank account in an EU Member State or EEA;
- Have proven experience in using English as a working language;
- Have minimum 3 years of demonstrable experience in the selected areas and fields of expertise;
- Have minimum 12 months of demonstrable experience in the selected areas and fields of expertise during the last 5 years;
- A motivation letter (500 words maximum), which establishes your incentive to be accepted as an expert for ENISA, as well as the capability of the applicant to work with others in a multicultural environment;
- CV preferably in Europass format.

The evaluation committee may exceptionally further consider candidates who are close to the minimum requirements for years of experience or who have a unique skillset, for inclusion in the List.

## 12. SELECTION CRITERIA

The selection of members is based on a personal capacity and a clear demonstrable skillset or research capacity in areas such as cybersecurity and market analysis.

In the assessment of the applications, ENISA will take into consideration the following criteria:

- Relevant competence (e.g., economic, technical, legal, organisational, statistical, or a combination thereof) related to market analysis and monitoring;
- Knowledge of the EU and/or national and/or international cybersecurity market;
- Knowledge of the cybersecurity requirements for placing on the market products with digital elements;
- Ability to deliver practical advice on issues related to the cybersecurity market;
- Ability to deliver advice of scientific nature regarding cybersecurity market analysis and monitoring methods;

- Ability to provide practical advice on existing data sources relevant to the analysis and monitoring of the EU cybersecurity market;
- Good presentation skills and public speaking, so as to act as an ambassador of the ENISA work in cybersecurity market and in cyber resilience, and ability to customise the message based on various stakeholder target groups;
- Good knowledge of English allowing for active participation in discussions, and drafting skills for written contributions to deliverables.

## 13. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA as appropriate against the selection criteria mentioned above under Section 12 (Selection criteria) of the Call, followed by the establishment of a list of the most suitable experts and concluded by the appointment of the members of the AHWG by the Executive Director of ENISA.

## ANNEX 1

### DECLARATION OF HONOUR ON EXCLUSION CRITERIA (FOR THE CANDIDATES WISHING TO BE FOR ADDITIONAL TASKS AS REMUNERATED EXPERTS)

Name:

"I hereby solemnly declare that I am not in one of the following situations:

#### I – SITUATION OF EXCLUSION CONCERNING THE PERSON

(1) <b>declares that</b> the above-mentioned person is in one of the following situations:	YES	NO
(a) it is bankrupt, subject to insolvency or winding-up procedures, its assets are being administered by a liquidator or by a court, it is in an arrangement with creditors, its business activities are suspended or it is in any analogous situation arising from a similar procedure provided for under EU or national laws or regulations;	<input type="checkbox"/>	<input type="checkbox"/>
(b) it has been established by a final judgement or a final administrative decision that the person is in breach of its obligations relating to the payment of taxes or social security contributions in accordance with the applicable law;	<input type="checkbox"/>	<input type="checkbox"/>
(c) it has been established by a final judgement or a final administrative decision that the person is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the		

person belongs, or by having engaged in any wrongful conduct which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence, including, in particular, any of the following:		
(i) fraudulently or negligently misrepresenting information required for the verification of the absence of grounds for exclusion or the fulfilment of selection criteria or in the performance of a contract or an agreement;	<input type="checkbox"/>	<input type="checkbox"/>
(ii) entering into agreement with other persons with the aim of distorting competition;	<input type="checkbox"/>	<input type="checkbox"/>
(iii) violating intellectual property rights;	<input type="checkbox"/>	<input type="checkbox"/>
(iv) unduly influencing or attempting to unduly influence the decision-making process to obtain Union funds by taking advantage, through misrepresentation, of a conflict of interests involving any financial actors or other persons referred to in Article 61(1) FR;	<input type="checkbox"/>	<input type="checkbox"/>
(v) attempting to obtain confidential information that may confer upon it undue advantages in the award procedure;	<input type="checkbox"/>	<input type="checkbox"/>
(vi) incitement to discrimination, hatred or violence against a group of persons or a member of a group or similar activities that are contrary to the values on which the Union is founded enshrined in Article 2 TEU, where such misconduct has an impact on the person's integrity which negatively affects or concretely risks affecting the performance of a contract or an agreement;	<input type="checkbox"/>	<input type="checkbox"/>
(d) it has been established by a final judgement that the person is guilty of the following:		
(i) fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995;	<input type="checkbox"/>	<input type="checkbox"/>
(ii) corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 and Article 3 of the Convention on the fight against corruption	<input type="checkbox"/>	<input type="checkbox"/>

involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997, and conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA, as well as corruption as defined in the applicable law;		
(iii) conduct related to a criminal organisation, as referred to in Article 2 of Council Framework Decision 2008/841/JHA;	<input type="checkbox"/>	<input type="checkbox"/>
(iv) money laundering or terrorist financing, within the meaning of Article 1(3), (4) and (5) of Directive (EU) 2015/849 of the European Parliament and of the Council;	<input type="checkbox"/>	<input type="checkbox"/>
(v) terrorist-related offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA, respectively, or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 4 of that Decision;	<input type="checkbox"/>	<input type="checkbox"/>
(vi) child labour or other offences concerning trafficking in human beings as referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council;	<input type="checkbox"/>	<input type="checkbox"/>
(e) it has shown significant deficiencies in complying with the main obligations in the performance of a contract or an agreement financed by the Union's budget, which has led to its early termination or to the application of liquidated damages or other contractual penalties, or which has been discovered following checks, audits or investigations by a contracting authority, the European Anti-Fraud Office (OLAF), the Court of Auditors or the European Public Prosecutor's Office (EPPO);	<input type="checkbox"/>	<input type="checkbox"/>
(f) it has been established by a final judgment or final administrative decision that the person has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95;	<input type="checkbox"/>	<input type="checkbox"/>
(g) it has been established by a final judgment or final administrative decision that the person has created an entity under a different jurisdiction with the intent to circumvent fiscal, social or any other legal obligations in the jurisdiction of	<input type="checkbox"/>	<input type="checkbox"/>

its registered office, central administration or principal place of business.		
(h) <i>(only for legal persons)</i> it has been established by a final judgment or final administrative decision that the person has been created with the intent provided for in point (g).	<input type="checkbox"/>	<input type="checkbox"/>
(i) for the situations referred to in points (c) to (h) above the person is subject to: <ul style="list-style-type: none"> <li>i. facts established in the context of audits or investigations carried out by the European Public Prosecutor's Office after its establishment, the Court of Auditors, the European Anti-Fraud Office (OLAF) or the internal auditor, or any other check, audit or control performed under the responsibility of an authorising officer of an EU institution, of a European office or of an EU agency or body;</li> <li>ii. non-final administrative decisions which may include disciplinary measures taken by the competent supervisory body responsible for the verification of the application of standards of professional ethics;</li> <li>iii. facts referred to in decisions of entities or persons being entrusted with EU budget implementation tasks;</li> <li>iv. information transmitted by Member States implementing Union funds;</li> <li>v. decisions of the Commission relating to the infringement of Union competition law or of a national competent authority relating to the infringement of Union or national competition law; or</li> <li>vi. informed, by any means, that it is subject to an investigation by the European Anti-Fraud office (OLAF): either because it has been given the opportunity to comment on facts concerning it by OLAF, or it has been subject to on-the-spot checks by OLAF in the course of an investigation, or it has been notified of the opening, the closure or of any circumstance related to an investigation of the OLAF concerning it.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>

**Name and Surname:**

**Date:**

**Signature:**