TLP-CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Call for Applications: Security Architecture Engineering and Vulnerability Management Ad-Hoc Working Group

FEBRUARY 2026

1. Introduction

The Security Architecture Engineering and Vulnerability Management Ad-Hoc Working Group (SAE & VM AHWG) will aim at supporting ENISA in achieving its objectives in the areas of security architecture and engineering for digital products and services, and on developing and maintaining a robust EU vulnerability management capacity[1].

The group will aim to support ENISA's activities in:

- putting forward analyses, recommendations and good practices that ensure appropriate cybersecurity levels of digital products and services during their planning, design, development, and maintenance;
- the maintenance of the EU Vulnerability Database, its cooperation with the Common Vulnerabilities and Exposures (CVE) Program[2], and potential other activities that contribute to serving its stakeholders and providing the expected value based on a delivery of matured services. Specifically, the mentioned activities need to be supported by building and developing relationships with producers (product vendors, Product Security Incident Response Teams (PSIRTs), cloud service providers) and consumers of vulnerability advisories (national CSIRTs, network owners, security service providers), as well as entities facilitating research in the area and fostering their exchange and potential alignment on vulnerability disclosure, assessment, management, and related efforts.

The SAE & VM AHWG will support ENISA with delivering reliable and continuous advice and support as per its mandate and annual work program, while additionally supporting activities related to pertinent EU cybersecurity initiatives and law. The AHWG will, inter alia, support ENISA to maintain an overview of related activities and foster the needed support for its activities.

The membership to the AHWG is foreseen to pursue broad, interdisciplinary representation across stakeholders' communities and aims to bring together professionals from diverse sectors, including public and private organizations, academia, civil society, and cybersecurity experts. It will serve as a platform for collaboration and knowledge-sharing, while supporting ENISA to deliver its mandate.

[1] As stipulated by 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 (NIS2 Directive), in particular its Art. 12(2).
[2] ENISA started maintaining a vulnerability registry service since becoming CVE Numbering Authority (CNA) in January 2024 and onboarding as a CVE Program-Root in November 2025, thus becoming a central point of contact within the CVE program for national/EU authorities, EU CSIRTs network members, and cooperative partners falling under ENISA's mandate.

2. Background

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 where necessary and within ENISA's objectives and tasks. Ad hoc working groups provide ENISA with specific advice and expertise. Prior to setting up an ad hoc working group, the Executive Director of ENISA shall inform the agency's Management Board.

The members of the ad hoc working groups 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[3].

Under Activity 5 (Provide effective operational cooperation through situational awareness) of the Agency's Single Programming Document 2026-2028, ENISA seeks to support operational cooperation within the CSIRTs Network and EU-CyCLONe, provide at their request advice to a specific cyber threat, assist in the assessment of incidents and vulnerabilities while facilitating technical handling of incidents. Furthermore, ENISA is tasked to analyse vulnerabilities, including through the EU Vulnerability Database established under NIS2 Directive [4] and the Single Reporting Platform established under the Regulation (EU) 2024/2847 (CRA)[5] while being able to deliver vulnerability services for EU stakeholders and participate in the CVE Program, namely the work related to the CVE Root and participation in the CVE governance structures.

Under Activity 8 (Supporting market, technology and product-security) of the Agency's SPD 2026-2028, ENISA seeks to promote and implement 'security by design' and 'security by default' measures in emerging technologies and in digital products and services. Furthermore, the activity aims to support the development of good cybersecurity engineering practices for products, services and technologies in direct support of ENISA role in CRA implementation, notably in terms of technical guidance and collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements and security updates.

Following the rationale described above, ENISA plans to facilitate and empower the communication and joint actions between the involved entities, as well as serve as a facilitator of communication between the targeted communities ranging from Member State public bodies to product vendors, research and civil society representatives. The experts chosen shall be well experienced in the subject and committed and motivated to participate in the exchange of information between European stakeholders that support ENISA with the mapping of relevant activities and validation of gaps, and contribute to building synergies that help bringing existing vulnerability management initiatives forward[6].

[3] Recital 59 of the Regulation (EU) 2019/881.
[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 (NIS 2 Directive), available under http://data.europa.eu/eli/dir/2022/2555/oj.
[5] 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) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), available under http://data.europa.eu/eli/reg/2024/2847/oj.
[6] While the collaboration with EU CSIRTs Network (CNW) members is continuous and dynamic, it is important to note that the AHWG to be established intends to develop a coherent approach towards additional stakeholders and partners.

3. Scope

The Security Architecture Engineering, and Vulnerability Management Ad-Hoc Working Group (SAE & VM AHWG) will cover two areas of work, including Security Architecture Engineering (SAE) and Vulnerability Management (VM) related services.

The first work area is meant to provide support, guidance and recommendations to ENISA efforts in the areas of promoting and implementing 'security by design' and 'security by default' measures through appropriate technical and organizational cybersecurity levels of digital products and services during their planning, design, development, and maintenance. Examples of activities that the members of this group might undertake in this context include:

- Identification of emerging and/or significant topics related to security architectures and engineering throughout the lifecycle of a digital product or service;
- Provide guidance on how to analyse these topics in order to achieve predefined goals, identify existing good practices and relevant European or International initiatives;
- Support drafting and analyses of good cybersecurity engineering practices for products, services, and technologies;
- Deliver input to and review documentation and recommendations related to ENISA activities and outputs in the areas of promoting and implementing 'security by design' and 'security by default';
- Contribute to the validation of outputs in relation to promoting and implementing 'security by design' and 'security by default';
- Advise ENISA in carrying out its tasks in support of Cyber Resilience Act[5] implementation, including promoting good cybersecurity engineering practices for products, services, and technologies, as well as addressing cybersecurity aspects related to privacy and data protection;

Via a second work area, the AHWG will support ENISA efforts in vulnerability communication provisions under relevant Union law in the cybersecurity domain and in relation to developing a robust EU vulnerability handling and management capacity in support of enhanced identification, assessment, and mitigation of security weaknesses in digital products. The AHWG will inter alia support ENISA to maintain an overview of related activities and foster the needed support for its activities and services.
Key objectives in this area include engagement in support of specific activities already initiated by ENISA, e.g.:

- Contribute to minimizing the delta between the publication and mitigation of vulnerabilities by further improving the vulnerability information provided via ENISA's EU Vulnerability Database service and its accessibility;
- Peer review ENISA's participation in international vulnerability regimes (in combination with its participation in the CVE Program) and driving the implementation of standardisation efforts

as well as further possible objectives, e.g.:

- Support the analysis of the threat level associated with common weaknesses initially leading to digital product vulnerabilities, enhancing situational awareness about exploitation trends, and

enabling the enrichment and contextualization of vulnerability data with the purpose of making it accessible;

- Review of sector specific initiatives in relation to vulnerability management, such as the creation of better situational awareness / documentation, fostering knowledge sharing and enabling an appropriate response in specific product categories (e.g., medical product, industrial control system, cloud service vulnerabilities).

The initial estimate of the duration of the ad hoc working group is for up to three (3) 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. Annually, a total workload of up to ten (10) Person-Days[7] is foreseen according to the role each member will undertake. The frequency of interaction will be decided between ENISA and the members of the group.

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

[7] A person-day is a unit of measurement representing the amount of work one person performs in a standard eight-hour workday.

4. Selection and appointment of members and observers

4.1 CONDITIONS FOR MEMBERS

Composition: The AHWG will be composed of up to **25** selected members-leading experts, based on the requirements of this open call[8].

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 from the cybersecurity field in the private, academia, and civil society organisations. It is expected that experts will be assigned to either of the work areas of the AHWG, namely Security Architecture Engineering and Vulnerability Management.

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 an initial cohort of up to **25** 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 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.

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. Appointed members who change affiliation shall inform ENISA accordingly, so that an informed decision about their further participation into the AHWG can be taken.

Replacement: 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 Group and may be replaced for the remaining duration of the ad hoc working group.

4.2 CONDITIONS FOR OBSERVERS

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

[8] 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.

Certain categories of observers may participate in the activities of the AHWG without undergoing a formal selection procedure. These include:

- Representatives of EU Institutions, bodies, offices, and agencies (EUIBAs);
- Public authorities of Member States and EEA/EFTA countries;

These participants serve as observers who may participate in the activities of the AHWG, but are not considered appointed members of the AHWG. Accordingly, they are not eligible for reimbursement of expenses under the provisions outlined in Section 8 of this call.

Moreover, as foreseen in Article 4(4) of the Decision No MB/2022/5 of ENISA Management Board, 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.

5. Organisation of the Ad Hoc Working Group

ENISA staff will be designated by the Agency's Executive Director as Chairperson and, if deemed necessary, as Vice Chairperson(s) of the AHWG. The Secretariat of the AHWG will be also provided by ENISA. The Chairperson shall be responsible for convening meetings, managing the agenda, coordinating the timely distribution of relevant information and documents, and addressing all organisational matters to ensure the effective operation of the AHWG. Meeting agendas will be distributed no later than four (4) working days prior to each meeting of the AHWG.

The AHWG may have Rapporteur(s) who ensure that draft reports or opinions are prepared, if necessary, within a set of time period. The work of the Rapporteur is terminated when the AHWG adopts the report or opinion.

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

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 Group on the basis of their interest and expertise.

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.

A minimum of 4 meetings per calendar year are foreseen and, in addition to the meetings, a minimum of four days of active engagement is also foreseen.

6. CONFIDENTIALITY,DECLARATIONS OF INTEREST AND IPR

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[9].

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 extend 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, the AHWG members may disclose their membership in this AHWG to the public and describe the general scope of the work of the AHWG.

In addition, the members, observers and any experts participating in a meeting of the AHWG are subject to the obligations of Article 25(2) of Regulation (EU) 2019/881 to declare any interests which could be considered to be prejudicial to their independence with respect to any of the points on the agenda. Moreover, members appointed to the AHWG shall submit their annual declarations of commitment and annual declarations of interest.

Participants of the AHWG will be requested to report, at the kick-off meeting of the AHWG or during the operation of the AHWG, if they have knowledge of Intellectual Property Rights (IPR related to the subjects discussed.
Inputs by AHWG members and observers which involve IPR will only be considered in duly justified cases. In such cases, AHWG members and observers shall explicitly declare the relevant IPR to ENISA in accordance with the applicable ENISA's IPR Policy[10].

If AHWG members and observers do not bring forward any IP right, or timely changes related to these rights, they cannot hold the Agency responsible for the consequences of the (re)-use of the material and possible subsequent IP right infringements of these parties.

[9] 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 under: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049.
[10] ENISA IPR POLICY

AHWG appointed members so as permanent and invited observers shall also abide by the ENISA policy related to usage of Artificial Intelligence (AI) in ENISA's work. They shall always acknowledge the use of AI tools in the work produced and specifically indicate the content (including graphics or images) that has been created by the use of AI.

7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[11]. For further information, please refer to the data protection notice that is available as a separate document with the call.

[11] 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 under http://data.europa.eu/eli/reg/2018/1725/oj.

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.[12]
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[13] 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.

Members designated by Member States and industry associations' representatives may be reimbursed upon submitting a request to ENISA.

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[14] The 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)[15] 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[16].
- The annual remuneration of a single expert shall in principle not exceed 30.000 euro.

[12] 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.
[13] 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
[14] CEI List of Individual External Experts to Assist ENISA | ENISA
[15] Regulation - EU, Euratom - 2024/2509 - EN - EUR-Lex.
[16] 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.

- The maximum amount of fees that can be paid to a single expert shall be 90 000 euro 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 members

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[17], 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.

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 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.

The expression of interest must be addressed to the Executive Director of ENISA and sent to saevm_ahwg@enisa.europa.eu. Following the review, the Executive Director may accept the participation of the organisation and their representative as observer of the working group.

This application process is intended for public entities and stakeholder organisations other than those falling under the categories listed in section 4.2, which may designate their representatives to the AHWG directly to the Chairperson. These entities are expected to maintain an up-to-date list of their designated representatives to ensure continuity and accuracy over time.

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'[18].

9.3 Deadline for application

The duly completed applications must be submitted **by 15 April 2026 at 12:00 EET (Athens time zone)**. 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.

[17] https://ec.europa.eu/eusurvey/runner/sae-ahwg-application.
[18] 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, See Art. 4 par. 3.

This deadline does not apply to entities referred to in Section 4.2, 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.

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 ad hoc working group 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;
  (Individuals without a bank account in an EU MS or 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 proven experience in using English as a working language;
- Have minimum 3 years of experience in the selected areas and fields of expertise;
- Have minimum 12 months of 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 become a member of the AHWG;

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

ENISA will take the following criteria into account when assessing applications:

- Relevant competence(s) (e.g., technical, legal, organisational or a combination thereof) related to Security Architecture Engineering and/or Vulnerability Management and related services;
- Prior knowledge and participation to EU and/or national and/or international initiatives related to Security Architecture Engineering and/or Vulnerability Management;
- Ability to deliver practical advice and recommendations on issues related to Security Architecture Engineering and/or Vulnerability Management and related elements for digital products and services;
- Good knowledge of English allowing for active participation in discussions, and drafting skills for written contributions to deliverables.

ENISA promotes equal opportunities and accepts applications without any concern on grounds of sex, racial or ethnic origin, religion or belief, age or sexual orientation, marital status or family situation.

The composition of the AHWG will strive for gender balance depending on applications likely to be received. Applications from disabled candidates are encouraged.

For a balanced composition of the AHWG ENISA will take into account also other factors such as geographical spread of representation, coverage of different sectors of the classical economy, personal experience, ability to liaise with the target community they represent, balance among selected members to cover both experience in cybersecurity supply (vendors) and demand (users of cybersecurity products, processes and services) and knowledge of the various critical segments and sectors in the market (both demand and supply sides).

The members of ad hoc working groups 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 (including SMEs), users, and academic experts in network and information security with knowledge on the functioning of the cybersecurity market.

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), followed by the establishment of a list of the most suitable applicants and concluded by the appointment of the members of the AHWG by the Executive Director of ENISA.

ANNEX I 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) **declares that** 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;	☐	☐
(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;	☐	☐
(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 credibity 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;	☐	☐
(ii) entering into agreement with other persons with the aim of distorting competition;	☐	☐

(iii) violating intellectual property rights;	☐	☐
(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;	☐	☐
(v) attempting to obtain confidential information that may confer upon it undue advantages in the award procedure*;*	☐	☐
(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;	☐	☐
(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;	☐	☐
(ii) corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 and Article 3 of the Convention on the fight against corruption 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;	☐	☐
(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;	☐	☐
(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;	☐	☐
(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;	☐	☐
(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);		
(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;	☐	☐
(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 its registered office, central administration or principal place of business.	☐	☐
(h) (*only for legal persons*) 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).	☐	☐
(i) for the situations referred to in points (c) to (h) above the person is subject to: 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; 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; iii. facts referred to in decisions of entities or persons being entrusted with EU budget implementation tasks; iv. information transmitted by Member States implementing Union funds; 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 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.	☐	☐

Name and Surname:

Date: **Signature:**

ANNEX II Abbreviations

CVE	Common Vulnerability Enumeration
CNA	CVE Numbering Authority
CSIRT	Computer Security Incident Response Team
KEV	Known Exploited Vulnerability
NIS2	Network and Information Security Directive
CSA	Cyber Security Act
CRA	Cyber Resilience Act
EUVD	EU Vulnerability Database

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union