



# Call for Expressions of Interest to Select Entities in Member States that Provide the Necessary Facilities to Enhance Existing or Host and Operate National Cyber Hubs

1. Introduction.....	1
2. Objectives of the National Cyber Hubs.....	2
3. About this call for expressions of interest (CfEI).....	4
4. Content of the applications.....	8
4.1. Submission forms.....	8
4.2. Key features of National Cyber Hubs.....	8
5. Eligibility and award criteria.....	10
6. Overview of the assessment and selection procedure.....	12
6.1. Assessment procedure.....	13
6.2. Selection.....	13
6.3. Communication.....	13
7. Tentative timetable.....	14
8. Procedure for the submission of expressions of interest.....	14
Annexes.....	16
List of abbreviations.....	17

## 1. Introduction

In a context of accelerated digitisation together with a growing number of cybersecurity incidents with increasing impact, in December 2020 the European Commission (EC) adopted the “EU cybersecurity strategy for the Digital Decade”<sup>1</sup>. Among other objectives, the cybersecurity strategy aims to improve capacities and cooperation to detect more cyber threats, more quickly, before they can cause large-scale damage.

The Russian invasion of Ukraine further underlines and reinforces the need to urgently step up cybersecurity capabilities at national and at EU level. This requires intensifying the exchange of information and improving detection of cybersecurity threats so as to promote better situational awareness and inform preventive and response actions.

The EU cybersecurity strategy envisages building, strengthening, and interconnecting, across the EU, security operation centres (SOCs) and cyber threat intelligence (CTI) capabilities for monitoring, detection and analysis, with the aim of supporting the detection and prevention of cyber threats and the provision of timely warnings to authorities and all relevant stakeholders.

Such cyber security capabilities are typically ensured by SOCs<sup>2</sup> of public and private entities, in combination with computer emergency response teams / computer security incident response teams (CERTs/CSIRTs) with the support of external, specialised sources of intelligence on cyber threats.

To implement this strategy, the previous DIGITAL work programmes (WP) for 2021-2022 and 2023-2024 included capacity- building for SOCs as well as actions supporting the creation of National Cyber Hubs, and networking them at European and EU level via cross-border SOCs and coordinating their activities to create a stronger SOC ecosystem, which included local and regional, private and public security operational centres for both horizontal and vertical sectors.

As specified in the Cyber Solidarity Act<sup>3</sup>, published in the official journal of the EU on 15 January 2025, it is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States’ and the Union’s preparedness and capabilities to prevent and respond to significant, large-scale and large-scale-equivalent cybersecurity incidents. The Cyber Solidarity Act provides, as part of the European Cybersecurity Alert System (ECAS), that a pan-European network of Cyber Hubs should be established, to build and enhance coordinated detection and common situational awareness capabilities. Support is also planned for the development and consolidation of the National Cyber Hubs and the Cross-Border Cyber Hubs, which were also financed previously and referred to as national SOCs/Cross-border SOCs.

The activities of the current work programme (2025-2027) build on the work already initiated in previous work programmes, where investment was made to support the creation of national SOCs and their interlinking via Cross-Border SOCs. While the Cyber Solidarity Act brings in new terminology – National Cyber Hubs and Cross-Border Cyber Hubs – as part of the European Cybersecurity Alert System, the current work programme aims to consolidate previous activities focusing on SOCs, with the continued objective of supporting joint actions to create an advanced (state-of-the-art) threat detection and cyber early warning ecosystem.

In this regard, under the EU’s ‘DIGITAL’ funding program, EUR 10 million are dedicated to “National Cyber Hubs” in the cybersecurity work programme (WP) 2025-2027.<sup>4</sup>

Where a Member State decides to participate in the European Cybersecurity Alert System, it must designate or, if necessary, establish a National Cyber Hub. These National Cyber Hubs should be able to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a cross-border Cyber Hub. This should serve to improve detection capabilities and ultimately the prevention of and response to cyber threats and incidents.

---

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>

<sup>2</sup> SOCs potentially cover any entity or team tasked with detecting and acting on cyber threats.

<sup>3</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202500038](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202500038)

<sup>4</sup> [https://cybersecurity-centre.europa.eu/document/a35f7be2-4464-43d3-a40f-6ec942036f48\\_en](https://cybersecurity-centre.europa.eu/document/a35f7be2-4464-43d3-a40f-6ec942036f48_en)

***The purpose of this call for expressions of interest (CfEI) is to select entities in EU Member States and other eligible countries<sup>5</sup>, intending to participate in the European Cybersecurity Alert System and willing to deploy and manage National Cyber Hubs.***

***The single entity, designated or established as the National Cyber Hub, selected following this CfEI will engage in and manage a joint procurement with the ECCC to purchase the necessary tools, infrastructures and services to create or strengthen the National Cyber Hub. For each joint procurement the EU will contribute up to 50% of the purchasing costs. The number of joint procurements to be conducted will depend on the number of successful applications from National Cyber Hubs selected following evaluation of this CfEI. The overall budget for procurement will be up to EUR 3 million.***

***Separately, a platform has to apply to receive a grant to complement the joint procurement(s). The related grant will be awarded if the relevant requirements in the separate call for proposals are met and only if the application in response to this call for expressions of interest is successful. The EU will contribute up to 50% of eligible costs, such as staff costs or other eligible costs for enhancing existing or setting up and running the National Cyber Hub, its interaction and cooperation with other stakeholders, with the exception of those tools, infrastructures and services that will be purchased through the joint procurement(s). The grant funding for the eligible costs of the National Cyber Hubs will come from the call for proposals on National Cyber Hubs, for which there is a total amount of EUR 2 million.***

**The deployment of these national platforms is a pivotal component in a wider strategy and set of actions** aimed at the stepping – up of monitoring and detection capabilities and the improvement of situational awareness at national, cross-border and EU level, and at paving the way for building a **collaborative, interoperable and sustainable pan-European network of infrastructure**. The network of infrastructure will link Cyber Hubs designated at national level forming several cross-border Cyber Hubs, which will be able to build up shared capacities and exchange information among themselves. Such platforms would together constitute a pan-European network of infrastructure.

Cooperation and exchange of information will be encouraged among the various entities at all levels through the **procurement of common equipment, software and services**, the development of **cooperation frameworks** and of specific conditions to ensure a high level of **interoperability** among the supported projects and infrastructures, which will fit into a **common, high-level blueprint architecture**.

**In this regard, National Cyber Hubs must share information with other stakeholders in a mutually beneficial exchange of information and commit to applying to participate in a cross-border Cyber Hub within the next 2 years from the date on which the tools, infrastructures and services were acquired, or which it received grant funding, whichever occurred sooner, with a view to exchanging information with other National Cyber Hubs.**

## **2. Objectives of the National Cyber Hubs**

The **general objective** of “**National Cyber Hubs**” is to act as reference points and gateways to other public and private organisations at national level for participation in the European Cybersecurity Alert System and to ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner.

National Cyber Hubs are public entities given the role at national level to act as clearinghouses for detecting, gathering, aggregating and storing data on cybersecurity threats, analysing this data, and sharing and reporting cyber threat intelligence (CTI), reviews and analyses. They provide a central operational capacity and support other SOC's at national level (e.g., by offering guidance or training, making available data or analysis of this

---

<sup>5</sup> EEA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States

data, coordinating joint detection and monitoring actions, providing incident response services methodologies towards the mitigation of identified threats, vulnerabilities and/or misconfiguration weaknesses). They will play a central role at national level and can act as a hub within a context of SOC's in the different countries.

The platforms should act as a central national point allowing for broader pooling of relevant data and CTI, enable the large scale dissemination of threat information on a large scale and among a large and diverse set of actors (e.g., CERTs/CSIRTs, ISACs, operators of critical infrastructures).

National Cyber Hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI. They will support the development of better performing data analytics, detection, and response tools, through the pooling of larger amounts of data.

**The National Cyber Hubs** should achieve this general objective through the following specific objectives:

- **Producing high quality, actionable information and CTI** through the use of state-of-the art tools and advanced tools and technologies (for example artificial intelligence (AI), including machine learning (ML) tools) on the large data sets of collected CTI.
- **Contributing to better detection and response to threats.** They should support quicker detection of cyber threats and incidents and more effective action plans and responses by relevant entities.
- **Contributing to collective situational awareness.** The platforms should contribute to the strengthening of the EU's common situational awareness and enhanced coordinated detection capabilities by sharing information at three levels:
  - At national level. Close and coordinated cooperation between public and private entities is central to strengthening the EU's resilience in the cybersecurity sphere. National Cyber Hubs could strengthen cooperation and information sharing between public and private entities and, as part of this, request and receive specific information where appropriate and in accordance with national and EU law. Different levels of sharing and integration of data and tools can be envisaged, ranging from the exchange of intelligence feeds and indicators of compromise (IoC) to more contextualised or sophisticated information on threats, incidents, and vulnerabilities.
  - Between National Cyber Hubs. National Cyber Hubs must share information with other National Cyber Hubs and commit to applying to participate in a cross-border Cyber Hub within the next 2 years. Conditions for exchanging information with other platforms are to be established. As per the political agreement on the Cyber Solidarity Act to be published in autumn 2024, entities participating in the European Cybersecurity Alert System should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels, a minimum level of application layer security, situational awareness dashboard and indicators.
  - With relevant EU entities and networks. Platforms should provide an adequate level of information to responsible networks and entities at EU level, in defined situations (such as in case of major incidents) and subject to appropriate conditions, in order to support common situational awareness and effective crisis management and response. In particular, platforms should support the exchange of relevant data and information with relevant sectoral and cross-sectoral communities, including relevant industry information sharing and analysis centers ('ISACs'). If the National Cyber Hub is not the competent authority designated or established by the relevant Member State under Directive (EU) 2022/2555, it is crucial that it coordinates with that competent authority in respect of such data requests and receipt.
- **Improving EU technological sovereignty.** The platforms should enhance the EU's cyber-threat knowledge base, support the development and improvement of EU tools, and help create and structure a European ecosystem for sharing CTI.
- **Providing other services and activities.** Such services and activities could include the sharing of tools (including commonly procured tools), the creation of one or more data lakes, the provision of cyber range services, and/or the training of cybersecurity analysts. These services could be offered, for

example, to the SOC network at national level, national critical infrastructures in the public and private sectors, CSIRTs, ISACs and where possible, to the wider EU cybersecurity community, including EU industry and research and academia.

- **Contribution to the surveillance and protection of critical undersea infrastructure:** Cross-Border Cyber Hubs could also deploy solutions for the surveillance and protection of critical undersea infrastructure, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications. The response to such hybrid threats could also include situational awareness performed through the collection and analysis of in-situ, sea-based sensor data as well as relevant satellite imagery. For this activity, operational synergies with the EU Copernicus Space Programme and in particular with its Security Service are required.

### **3. About this call for expressions of interest (CfEI)**

The purpose of this CfEI is to select entities in the Member States that can provide the necessary facilities to enhance existing or host and operate the National Cyber Hub. The call for expression of interest will also build up the planning and design of necessary tools, infrastructures and services to be jointly purchased.

#### **3.1 Selection of National Cyber Hubs**

##### **3.1.1 Selection of New National Cyber Hubs**

This CfEI intends to select entities **designated or established by the Member States as National Cyber Hub**.

For the purpose of this CfEI, a national SOC is understood to be a public body that acts as a central hub, having the operational capacity to act as a reference point and gateway to other public or private organisations that themselves have significant capacities to produce, share, receive and analyse cybersecurity related data (e.g., operators of critical infrastructures, cybersecurity companies), or organisations that benefit from the services of the national SOC. The National Cyber Hub may be a CSIRT, or where applicable, a national cyber crisis management authority or other competent authority designated or established under Directive (EU) 2022/2555, or another entity.

Hosting and usage agreements will be signed between the selected National Cyber Hubs and the ECCC regulating the usage of the tools, infrastructures and services.

While the applicants under this CfEI are the entities designated or established by the Member States as National Cyber Hub, identification and engagement of the relevant stakeholders should be envisaged. To this end, National Cyber Hubs should aim at involving a large number of **contributors**, i.e. entities willing to contribute to the objective of the platforms, in particular by sharing data and tools, but without a direct link to the governance and operation of the platforms. The relevant contributors for a National Cyber Hub could be, among others: sectoral SOC, national decision and policy makers as well as other governmental and non-governmental organisations, law enforcement, academic, research and innovation communities, private sector including the sectors of essential and important entities according to the NIS2 Directive.

While the European Cybersecurity Alert System is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructures.

##### **3.1.2 Enhancement of existing National Cyber Hub**

**Previous calls for expressions of interest** were launched to select entities in EU Member States and other eligible countries, willing to deploy and manage National Cyber Hub platforms. The selected consortia have already engaged in joint procurement agreements with the ECCC to purchase the necessary tools, infrastructures and services to establish/enhance the Cross-Border Cyber Hub platforms.

As the previous CfEIs launched may be viewed as a first phase for the selected beneficiaries, it may be necessary to evolve the platform(s) in a subsequent phase, with the aim of better achieving the objectives listed under Section 2 above. In this regard, existing consortia can increase and reinforce the capabilities of the platforms.

This CfEI intends to allow the existing consortia to apply for phase 2 of the project for the enhancement of the capabilities of the National Cyber Hub platforms. If the expression of interest of phase 2 is successful, the hosting and usage agreement and the joint procurement agreement signed between the ECCC and the coordinator of the hosting consortium may be amended upon ECCC request. This will not affect the ECCC's ownership rights over the tools, infrastructures and services already jointly procured with that hosting consortium.

### **3.2 Overview of the process**

In response to this CfEI, applicants should submit a proposal that explains how the National Cyber Hub will be created or strengthened. The application should explain in detail the goods and services that the participating national SOC intends to jointly procure with the ECCC in order to create or strengthen the National Cyber Hub.

To this end, each application should provide a detailed description of the proposed approach using the submission forms attached to this document:

- the submission form on 'information about the applicant' in Annex 1
- the submission form for the expression of interest related to the joint procurement(s) in Annex 2.

The submission of an expression of interest to engage in joint procurement with the ECCC for the purchase of goods and services necessary to create or strengthen a National Cyber Hub will be evaluated using the evaluation criteria established in this document.

Separately, applicants have to submit a proposal for a grant to fund running costs and other costs of the National Cyber Hub, which will be evaluated using the evaluation criteria established in the relevant call document under the Digital Europe Programme<sup>6</sup>.

The procedure for creating or strengthening a National Cyber Hub with the support of funding provided under this call for expressions of interest and the relevant call for proposals<sup>7</sup> will be as follows:

1. This call for expressions of interest will lead to the selection of applicants intending to create or strengthen a National Cyber Hub.
2. Before launching the procedure for the acquisition of the tools, infrastructures and services, the ECCC and the National Cyber Hub/national SOC will conclude a hosting and usage agreement. This agreement will set out practical arrangements for managing the hosting and usage of the tools infrastructures and services co-owned by the ECCC and the participating national SOC after joint procurement has been carried out.
3. Each selected National Cyber Hub/national SOC will take part in joint procurement of goods and services with the ECCC. Several parallel joint procurements procedures may thus be launched depending on the number of successful applications to CfEI. To this end, the ECCC and each selected Member State will sign a joint procurement agreement setting out the practicalities of the procurement procedure.
4. The National Cyber Hub/national SOC will also apply for a complementary grant, to cover eligible costs, such as the cost of setting up and running the National Cyber Hub. To be eligible for such a grant, applicants must submit a proposal for a grant in response to the relevant [call for proposals](#) opened on 9 December 2025 following the procedure established for that purpose.

By submitting an application in response to the CfEI, the National Cyber Hub/national SOC agrees to the terms and conditions set out in the model hosting and usage agreement. The model hosting and usage

---

<sup>6</sup> See section DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs in the [call fiche DIGITAL-ECCC-2026-DEPLOY-CYBER-10](#)

<sup>7</sup> See section DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs in the National Cyber Hubs in the [call fiche DIGITAL-ECCC-2026-DEPLOY-CYBER-10](#)

agreement is found in Annex 3 to this CfEI. The model hosting and usage agreement may be further modified before the close of the call for expressions of interest, subject to further discussions with Member States.

**Member States willing to create or strengthen existing National Cyber Hubs will be selected through this call for expressions of interest.**

**For the joint procurement(s), the EU financial contribution is estimated at a maximum of EUR 3 million for all selected National Cyber Hubs. The EU contribution would cover up to 50% of the purchasing costs of the tools, infrastructures and services. The remaining procurement costs would be covered by the Member State. The EU contribution can only be used for jointly purchased goods and services.**

**In addition, Member States have to apply for a grant to cover other costs through a separate call for proposals<sup>8</sup>. The EU funding rate for such a grant is 50%.**

**Successful applicants to both workstreams (call for expressions of interest and call for proposals) will engage in joint procurement with the ECCC to purchase the necessary tools, infrastructures and services to create or strengthen the National Cyber Hubs.**

**To that end, the ECCC will conclude a hosting and usage agreement only with the National Cyber Hubs that are selected following this CfEI and that have been awarded a grant under the call DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs. This condition is cumulative.**

#### ***Joint Procurement(s)***

The financial rules of the ECCC, adopted through DECISION No GB/2024/3<sup>9</sup> of the ECCC Governing Board, set out the conditions under which the ECCC may engage in procurement, including joint procurement with the Member States.

Joint procurement(s) for tools, infrastructures and services to create or strengthen National Cyber Hubs will be carried out by the ECCC in accordance with the ECCC financial rules and using the ECCC procedural provisions. The ECCC will jointly acquire, with each National Cyber Hub/national SOC selected further to the CfEI, relevant components of a National Cyber Hub and will co-own them with the participating Member State that provides a share of the funding. Share of ownership will correspond to share of the funding provided.

Considering that the Member State's financial contribution to the acquisition of the tools, infrastructures and services will represent at least 50% of the total acquisition cost, and based on an assessment of the complexity of the needs and the Member State's capacity to carry out the procurement procedure, the ECCC may decide at a later stage, not later than the signature of the joint procurement agreement and hosting and usage agreement, whether the joint procurement shall follow the procedural rules of the ECCC or those of the Member State, in accordance with Article 158(2) of the Financial Regulation. In case the procedural rules of the Member State will be used, the ECCC will authorise the National Cyber Hub to act on its behalf in accordance with the national public procurement provisions to conduct the joint procurement procedure including the award and signature of the contract, and to manage the resulting contract.

The designated or established National Cyber Hub will represent the Member State and be authorised to sign the hosting and usage agreement, the joint procurement agreement and subsequent amendments to both agreements, if needed. **Evidence of this designation must be provided as part of the application in response to the CfEI.**

Each Member State must commit to ensuring its individual share of the co-funding of at least 50 % of the overall estimated procurement costs not covered by the EU contribution and transferring it to the ECCC, when required. **Evidence of this commitment must be provided as part of the application in response to the CfEI.**

---

<sup>8</sup> [EU Funding & Tenders Portal](#)

<sup>9</sup> [https://cybersecurity-centre.europa.eu/system/files/2024-04/ECCC%20Decision%20GB%202024\\_3%20Financial%20Rules%20amended.pdf](https://cybersecurity-centre.europa.eu/system/files/2024-04/ECCC%20Decision%20GB%202024_3%20Financial%20Rules%20amended.pdf)



By submitting the application, applicants provide their prior acceptance with the terms and conditions set out in the model hosting and usage agreement. The model hosting and usage agreement is found in Annex 3 to this CfEI.

**As part of their application, applicants are required to supplement the model hosting and usage agreement by completing the part of the agreement that is specific to their application. In particular, applicants must submit as part of their application a completed version of the model hosting and usage agreement.**

Typical examples of goods and services to be procured include (indicatively):

- Hardware: servers, micro data center racks, high speed switches, firewall switches, GPUs, HSMs, probes;
- Software: visualisation tools, SIEM tools, vulnerability managers, aggregation tools, incident reporting tools, situation awareness correlator tools, AI/ML tools, PKI tools, orchestration systems;
- Services: CTI feeds, AI/ML functionality updates, dedicated service virtual telco line, cloud storage, software development and tuning services, consultancy services.

The objective is to encourage convergence among the various platforms and, as far as possible, to use procurement(s) to acquire goods and services that can benefit all the platforms by setting the path towards interoperability in the framework of cross-border cooperation and information exchange between the National Cyber Hubs. If duly justified, specific types of goods and services for individual platforms could also be included in the procurement(s).

### ***Rules for participation in DIGITAL Programme***

In accordance with the Digital Europe Regulation, the joint procurement to be carried out following this CfEI **is restricted in line with the rules for participation in the Digital Europe Programme (DEP)**. The conditions set out in Appendix 3 – Implementation of Article 12(5) Regulation (EU) 2021/694 to the work programme 2025 – 2027<sup>10</sup> apply in this regard.

### **3.3 Applications for complementary grants**

Separately from this call for expressions of interest, the selected National Cyber Hubs have to apply to be supported through grants awarded further to the call for grant proposals on National Cyber Hubs mentioned above. Procedures are described in the relevant call document<sup>11</sup>.

Examples of specific activities which may be supported under the grant are provided in the text of that call for grant proposals on creating or strengthening National Cyber Hubs<sup>12</sup>, whereas the eligible costs are defined in the general model grant agreement of the Digital Europe Programme.<sup>13</sup> Eligible costs may include the costs for maintenance or recurrent licences required for running the national SOC and which cannot be purchased as part of the joint procurement(s).

Grants may cover up to 50% of eligible costs of the selected National Cyber Hubs for setting up/strengthening a National SOC and running it.

Applications to receive such a grant must be submitted separately through the Funding and Tenders portal.<sup>14</sup>

Applications have to be made to both workstreams (call for expressions of interest for joint procurement and call for proposal for complementary grant). **Applicants to both workstreams must be the same entities**

---

<sup>10</sup> [https://cybersecurity-centre.europa.eu/document/a35f7be2-4464-43d3-a40f-6ec942036f48\\_en](https://cybersecurity-centre.europa.eu/document/a35f7be2-4464-43d3-a40f-6ec942036f48_en)

<sup>11</sup> See section DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs in the [call fiche DIGITAL-ECCC-2026-DEPLOY-CYBER-10](#)

<sup>12</sup> See section DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs in the [call fiche DIGITAL-ECCC-2026-DEPLOY-CYBER-10](#)

<sup>13</sup> [https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/agr-contr/mga\\_dep\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/agr-contr/mga_dep_en.pdf)

<sup>14</sup> [EU Funding & Tenders Portal](#)

**designated or established as National Cyber Hubs. Grants will only be awarded to applicants that have succeeded in the evaluation of the joint procurement action.**

Any application for a grant by entities also applying to this call for expressions of interest should be consistent with the application to engage in joint procurement under this call for expressions of interest, notably by ensuring complementarity and avoiding duplication of costs to be covered.

#### **4. Content of the applications**

##### **4.1. Submission forms**

Participants must fill in the submission forms in Annex 1 and 2 to describe their projects and enable their assessment.

**1) The first Annex “Information on the participant”** must provide administrative **details about the entity designated or established** by the Member State as National Cyber Hub/national SOC, including contact details and legal representatives.

**2) The second Annex (“Information on the expression of interest”)** relates to the Joint procurement(s) and should be completed with:

- A **description of the project and its relevance and impact**, according to the key features detailed below in Section 4.2. Participants are expected to describe each part according to the points indicated.
- Information about the total cost of acquisition. This should include detailed **information about the types of goods and services to be procured under the joint procurement(s) for the purpose of creating/strengthening the National Cyber Hubs and their projected costs**.
- Information about existing infrastructures and other resources offered by those replying to the CfEI.
- A short description of complementarity with the application for grants. Applicants should provide a summary of the grant part of the project and explain the link between the procurement and the grant parts, explaining how one complements the other and which aspects and costs they cover respectively.

##### **4.2. Key features of National Cyber Hubs**

This section describes the main features of the National Cyber Hubs, as background information when completing the submission form.

Several National Cyber Hubs will be selected following this CfEI, one in each Member State and other eligible countries. An appropriate level of synergies and collaboration will be required between them and/or with other national/cross-border platforms. In particular, the National Cyber Hubs should adopt consistent and interoperable approaches and standards, in order to allow for possible exchanges of information among them at a later stage and participation in a cross-border Cyber Hub, as appropriate. The requirements of the Cyber Solidarity Act should be observed in this regard. The platforms should be congruent with the high-level blueprint architecture available in Annex 5.

Specifically, the submissions should cover the following elements:

- **General concept and organisation.** This section should explain the overall vision for the platform, including its maturity and readiness to enhance existing or host and operate the National Cyber Hub. It should describe organisational aspects and demonstrate how these would enable increased data sharing and better detection capability for cyber threats. The overall setting should be designed to foster engagement and trust with other SOC's and relevant entities in the country. Proposals should also consider how the proposed platforms will help expand the EU's cyber threat knowledge base and make the EU more and technologically independent, also in view of a role in the cross-border platforms.
  - o **Minimum condition for the expression of interest.** As set out above, a National Cyber Hub should be managed by the single entity acting under the authority of a Member State designated or established as the National Cyber Hub (public entity acting as hub). This overall concept should constitute the common baseline for all submissions, however each platform

can, within that context, take into account their specific focus. Basic conditions for collaboration with the relevant identified stakeholders should be outlined in the submission. While the platforms will be managed by public entities, a concrete engagement from the private sector, or at least a clear strategy to engage with the private sector, should be demonstrated from the outset.

- **Objective to be achieved during the deployment phase.** A comprehensive governance framework should be developed. It should address data sharing (see below), security and access rights, collaboration conditions.
- **Interoperability of National Cyber Hubs at national and EU level:**
  - **Minimum condition for the expression of interest.** Standards and tools to be used within individual platforms should be described, and should be congruent with the common, high-level blueprint architecture described in Annex 5. The use of malware information sharing platform (MISP) and of the relevant state of the art IT tools is strongly recommended.
  - **Objective to be achieved during deployment phase.** Given that Cross-Border Cyber Hubs are required to agree on a single common data format and taxonomy and on a common data structure, to ensure interoperability and enable data sharing across platforms, National Cyber Hubs should also consider this choice in order to be ready for sharing or joining a cross-border consortium in the future. Other elements to consider include interoperable privacy preserving technologies, data handling tools, communication and security technology, and situation awareness dashboard and indicators.
- **Data management (level of data sharing, conditions and incentives and legal aspects)**
  - **Minimum condition for the expression of interest.** National Cyber Hubs should demonstrate a willingness to share as much information as possible with the due level of speed and quality. A general approach to data ownership and management, including legal aspects should be outlined. The approach should ensure “compliance by design” with respect to relevant EU and national legislations, in particular as regards rules on data protection and privacy.
  - **Objective to be achieved during deployment phase.** As part of the comprehensive concept and organisation framework referred to above, clear and appropriate rules of engagement should be drawn up so as to incentivise the various stakeholders/contributors to engage and share information. This should include detailed terms of reference, covering aspects such as data sharing (ownership, control, compliance, management), security and access rights. Also, engagement could be based on a set of indicators to measure stakeholder’s participation in terms of the amount of information shared, frequency, quality and type of information, and a set of corresponding rewards (e.g., access to more detailed info). If several platforms are selected the ECCC may invite them to share best practices, in which case they should join a working group to do so. Applicants are invited to include such tasks in the grant part of their proposal.
- **Contribution to national and EU-level situational awareness:**
  - **Minimum condition for the expression of interest.** The National Cyber Hub should be the national reference point for cybersecurity situational awareness. As outlined in the blueprint architecture in Annex 5, it is a single point of contact towards other National Cyber Hubs and the cross-Border SOC in which it may participate, thus contributing not only to the national but also to the EU common situational awareness and coordinated detection capabilities. To support situational awareness and effective crisis management and response, the National Cyber Hub should provide an adequate level of information to responsible networks and entities at national and EU level, in defined situations (such as in case of major incidents) and subject to appropriate conditions. To specify what situations and conditions should be taken into account, the National Cyber Hub should engage with other platforms and the EU level. The Cyber Hub needs to commit to apply to participate in a cross-border Cyber Hub within the next 2 years from the date on which the tools, infrastructures and services were acquired, or which it received grant funding, whichever occurred sooner.

- **Highly secure infrastructure and state-of-the-art technologies and tools:**
  - **Minimum condition for the expression of interest.** Candidates should describe dedicated secure infrastructure with the highest security standards. They should list equipment, software and services to be procured, which should include state-of the-art technologies, including notably AI/ML tools, based on a review of latest technologies available on the market. Proposals should be congruent with the common, high-level blueprint architecture described in Annex 5. With regard to secure communications, to ensure future interoperability across the different platforms, all candidates are invited to look at the suggested approach described in Section 4 of Annex 5. Proposals should also consider to what extent the proposed platforms will contribute to increase national and EU technological independence.
  - **Objective to be achieved during tender preparation phase.** The National Cyber Hubs selected following this CfEI will be required to commit sufficient resources and expertise work together with the ECCC on the preparation, launching, and management of the procurement procedures. For this, working groups could be set up to consider a common approach to identifying needs. This effort will aim at identifying common equipment, tools, etc. to be purchased through the joint procurement actions, where possible (also in view of National Cyber Hubs aiming to join new or existing cross-border platform). As regards security and secure communication channels, entities should commit to meeting very high standards (if necessary, in a gradual way), considering also putting in place measures for the future evolution of cryptographic implementations towards post-quantum cryptography.
- **Provision of other services and activities to strengthen national and EU detection capabilities:**
  - **Minimum conditions for the expression of interest.** Candidates should describe other activities and services that could be provided by the platform. Such activities and services could include the sharing of tools (including commonly procured tools), the creation of one or several data lakes to train tools, the provision of cyber range services, and/or training of cybersecurity analysts. Depending on the activities and conditions agreed on by platforms, these services could be offered to the SOC network at national level, and where possible, to the national and EU cybersecurity community, including industry and research and academia. In addition, links with existing and future relevant initiatives and projects benefiting from EU funding should be encouraged.
  - **Objective to be achieved during the deployment phase.** The National Cyber Hubs selected following this CfEI will be encouraged to work together with the relevant stakeholders/contributors to identify synergies between other services and activities provided by individual platforms and to create appropriate infrastructures to leverage the shared pool of knowledge among the national SOC network. For this, they could for instance explore the possibility of creating one or more data lakes (see Section 2 above).

## 5. Eligibility and award criteria

In order to be eligible, the expression of interest for the joint procurement(s) must satisfy all the conditions set out below:

### Expression of interest

1. The **expression of interest** must be submitted by the deadline given in Section 7, following the procedure set out in Section 8.
2. The **expression of interest** must be completed using the submission forms detailed in Annex I and Annex 24 addressing all mandatory aspects that are described in this document.
3. The **expression of interest** must be aligned with the objectives of this CfEI and fit into the expected approaches and elements of structure of National Cyber Hubs as described in Section 20.

4. The **expression of interest** must comply with the available budget detailed in Section 3.

#### **Member State public body submitting the expression of interest**

- 1 A National Cyber Hub must be represented for legal purposes, including for submitting the expression of interest, by the single public entity acting under the authority of a Member State designated or established as the National Cyber Hub/national SOC.
- 2 The applicant must have legal personality and must be designated by the Member State to act as National Cyber Hub/. **Each application must contain the relevant documents proving the legal status of the National Cyber Hub (e.g. designation letters, establishment act).**
- 3 Each Member State must provide a commitment to engage in a joint procurement action with the ECCC and to transfer the required acquisition costs. For this purpose, each application must contain copies of Annex 4 ('Commitment letter').

Failure to comply with those eligibility criteria will lead to disregarding the **expression of interest**.

**Award criteria:** Proposals must address all features indicated in this Section 0 and will be assessed accordingly, taking into consideration the criteria indicated below for each of those features.

#### **Award criteria for the expression of interest**

<b>Criterion</b>	<b>Score</b>
<b>General concept and governance:</b> <ul style="list-style-type: none"><li>• Quality of the vision, development plans and capability of the Member State to set up/strengthen and manage the National Cyber Hub and to create a trusted environment stimulating the active participation of and sharing with relevant stakeholders.</li><li>• Added value with relation to existing structures</li><li>• Contribution to the EU's technological independence (e.g., use of EU made solutions, EU sourced data)</li><li>• Sustainability of collaboration in the longer term</li><li>• Feasibility and credibility of the presented approach</li></ul>	0-20 points
<b>Feasibility and quality of the interoperability:</b> <ul style="list-style-type: none"><li>• Use of common data format and taxonomy</li><li>• Quality of the proposed approach for interoperability and trusted interaction and data exchange with the national SOC network, other National Cyber Hubs and relevant EU stakeholders. Use of international recognised standards, protocols, best practices and guidelines to guarantee interoperability with other Cyber Hubs, including other National Cyber Hubs, and commitment for cross-platform cooperation and/or integration plans.</li></ul>	0-15 points
<b>Highly secure infrastructure and state-of-the-art technologies and tools</b> <ul style="list-style-type: none"><li>• Quality and effectiveness of the proposed plan for the readiness of the site to enhance existing or host the system</li><li>• Security of the infrastructure</li></ul>	0-15 points

<ul style="list-style-type: none"> <li>• Use of most advanced technologies and tools based on market review</li> <li>• Compliance with the system specifications set out in this CfEI</li> <li>• Quality and pertinence of the current and proposed hosting facility's physical and IT infrastructure, its security, and its connectivity</li> <li>• Quality and pertinence of experience and know-how of the intended team that would be in charge at hosting entities for installing and running the platform</li> </ul>	
<b>Data management</b> <ul style="list-style-type: none"> <li>• Quality and effectiveness of proposed plan for data management (e.g., access rights, ownership, control)</li> <li>• Commitment to share information with identified stakeholders/contributors at national level</li> <li>• Mechanisms to encourage data sharing by all contributors to the platforms</li> <li>• Approach to legal aspects (e.g., compliance with legislation, anonymisation, etc.)</li> </ul>	0-15 points
<b>Contribution to EU-level situational awareness</b> <ul style="list-style-type: none"> <li>• Commitment to contribute to EU situational awareness and to engage with the EU level to define minimum level of sharing of information with responsible EU entities (and other platforms, upon agreement).</li> <li>• Feasibility and credibility of the proposed plan to apply for joining a cross – border Cyber Hub.</li> </ul>	0-15 points
<b>Provision of other services and activities to strengthen EU detection capabilities</b> <ul style="list-style-type: none"> <li>• Quality and effectiveness of the proposed services and activities to contribute to EU capabilities</li> <li>• Links with existing and future relevant EU-funded initiatives and projects</li> </ul>	0-10 points
<b>Goods and services to be procured and total cost of acquisition (TCA)</b> <ul style="list-style-type: none"> <li>• Suitability of proposed goods and services to be jointly procured to achieve the objectives of the National Cyber Hub</li> <li>• Clarity and effectiveness of the estimated TCA of the National Cyber Hub, focusing on the total cost of what will be needed to be procured under the joint procurement(s) to run the platform</li> </ul>	0-10 points

The threshold for each criterion is the 60% of the maximum available points attributed to the criteria itself. The total score will be calculated as the sum of the individual scores. The total maximum number of points is 100.

## 6. Overview of the assessment and selection procedure

The ECCC is responsible for assessing of the expressions of interest received. It will organise the submission and assessment procedures and communicate with those who submitted expressions of interest.

### 6.1. Assessment procedure

The submitted expressions of interest will be assessed in a procedure by a panel of ECCC staff and possibly assisted by independent experts. The ECCC will assess the eligibility and award criteria according to the sections above.

Only eligible expressions of interest will be assessed.

- Individual assessments. In the first step, each expression of interest will be assessed individually against the assessment criteria described in Section 5, receiving a score for each criterion, with explanatory comments. These scores and comments will be recorded in individual reports which form the basis for further assessment.
- Consensus meetings. After carrying out their individual assessment of the expressions of interest, the members of the evaluation committee will hold a consensus meeting, to agree on a common position, including comments and scores and prepare a consensus report.
- Panel review. The members of the panel will review the scores and comments for all expressions of interest to check for consistency across the assessments. If necessary, it will propose a new set of scores or revised comments and resolve cases where there are different views. The panel will prepare an assessment report, with its final ranking list and scores for the award criteria set out in Section 5. Only expressions of interest that score above threshold for each individual criterion will be ranked in order of the total score.
- Potential priority order. If necessary, a priority order for expressions of interest with the same score will be determined in the ranked list, according to the following approach: Expressions of interest with the same total score will be prioritised according to the scores they have received for the award criterion “*stakeholder engagement and Incentives*”. If these scores are equal, priority will be based on the scores for the award criterion “*data management*”. If these scores are also the same, the panel will decide on the method used to assign priority, such as one of the other award criteria or, if all scores are equal, on other aspects of the expressions of interest.

### 6.2. Selection

The Executive Director of the ECCC will review the results of the assessment panel and will approve a final ranking list based on the list proposed by the panel.

This final ranking list will consist of the expressions of interest to be selected as proposed by the panel and approved by the Executive Director.

In addition, the ECCC will draw up a list with expressions of interest that did not pass the assessment thresholds or were found to be ineligible.

Following his approval, the Executive Director will in due course inform the ECCC Governing Board and the DEP programme committee about the selected applicants.

After the decision of the Executive Director, those submitting expressions of interest will be informed in written by the ECCC of the outcome of the assessment. The ECCC will also inform about the final selection or rejection of both the expressions of interest and proposals for the complementary grants (Call: DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs).

The ECCC will subsequently invite the selected applicants to the next stages for the signature of the hosting and usage agreement, and the preparation of the joint procurement(s) of goods and services for national SOC platforms, including the signing of a joint procurement agreement. However, the invitation does not constitute a commitment by the ECCC to launch the procurement procedures. The hosting and usage agreement, the joint procurement agreement, or any amendments to either agreement, must be approved by the Executive Director before they are signed by the respective parties.

### 6.3. Communication

The call document provides all the information required to submit an expression of interest. Please read it carefully before doing so, paying particular attention to the priorities and objectives of the call.

Any enquiries must be made by e-mail only to: [applicants@eccc.europa.eu](mailto:applicants@eccc.europa.eu).

Questions on submission must be sent before the deadline indicated in Section 7. The ECCC has no obligation to provide clarifications to questions received after this date.

To ensure equal treatment of applicants, the ECCC will not give a prior opinion on the eligibility of applicants, affiliated entity(ies), actions or specific activities.

Questions will be replied to individually. Questions and answers of broad interest and other important notices will be published (FAQ in English) at regular intervals on the [European Cybersecurity Competence Centre website](#) under the relevant call.

The ECCC may, on its own initiative, inform interested parties of any error, inaccuracy, omission, or clerical error in the text of the CfEI on the mentioned website. It is therefore advisable to consult this website regularly to be informed of any updates and of the questions and answers published.

No changes may be made to the expressions of interest once the deadline for submission has elapsed. If there is a need to clarify certain aspects or to correct clerical mistakes, the ECCC may contact applicants for this purpose during the assessment process. This is generally done by e-mail. It is entirely the responsibility of the applicants to ensure that all contact information provided is accurate and functioning.

In case of any change of contact details, please send an email with the reference to the expression of interest and the new contact details to [applicants@eccc.europa.eu](mailto:applicants@eccc.europa.eu),

Applicants will be informed in writing of the results of the selection process. Unsuccessful applicants will be informed of the reasons for rejection. No information regarding the award procedure will be disclosed until the notification letter has been sent to the legal representative.

## 7. Tentative timetable

- 28 May 2026: deadline to submit expressions of interest to set up National Cyber Hubs and request for complementary grants under call DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs. **This deadline is definite, not tentative.**
- September 2026: finalisation of assessment of expressions of interest and grant application
- Q4 2026: signing of joint procurement/hosting and usage agreement
- Q1 2027: work with experts to draft technical specifications for joint procurement call(s) for tender
- Q2 2027: publication of joint procurement call(s) for tender by ECCC and National Cyber Hubs
- Q3 2027: signing of procurement contract with selected contractors

## 8. Procedure for the submission of expressions of interest

Expressions of interest for joint procurement and proposals for grants must be submitted before the call deadline **28 May 2026 17.00 hours CET** (see also timetable Section 7).

Expressions of interest must be submitted electronically via the ECCC website using the [application form](#) available on the website under the relevant topic. Paper submissions are NOT possible.

Expressions of interest (including annexes and supporting documents) must be submitted using the forms provided with this call for expressions of interest that can be downloaded from the [ECCC website](#) and/or the [application form](#). Section 4 provides information on how to fill in the submission forms.

Expressions of interest must be submitted in English, in the correct form, duly completed, and dated.

Your application must be readable, accessible and printable.

Proposals for grants must be submitted separately by responding to the [call for proposals](#) on the Funding and Tenders portal.<sup>15</sup>

---

<sup>15</sup> <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH>



Contact point for any questions is [applicants@eccc.europa.eu](mailto:applicants@eccc.europa.eu).

You have specific rights regarding processing of your personal data by the ECCC and the European Commission for the purpose of this call for expressions of interest. These rights are outlined in the [Data Protection Notice](#) available on the website under the relevant topic.

## **Annexes**

The annexes to this call for expression of interest are:

- Annex 1: **Information on the participant**
- Annex 2: **Information on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment letter**
- Annex 5: **Blue-print architecture**

The following four documents (Annex 1 to 4) must be filled by applicants:

- Annex 1: **Information on the participant**
- Annex 2: **Information on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment letter**

## **List of abbreviations**

<b>AI</b>	<b>Artificial Intelligence</b>
<b>CA</b>	<b>Certificate Authority</b>
<b>CEF</b>	<b>Connecting Europe Facility</b>
<b>CfEI</b>	<b>Call for Expression of Interest</b>
<b>CERT</b>	<b>Computer Emergency Response Team</b>
<b>CSIRT</b>	<b>Computer Security Incident Response Team</b>
<b>CTI</b>	<b>Cyber Threat Intelligence</b>
<b>DEP</b>	<b>Digital Europe Programme</b>
<b>ECCC</b>	<b>European Cybersecurity Competence Centre</b>
<b>EC</b>	<b>European Commission</b>
<b>ENISA</b>	<b>European Union Agency for Cybersecurity</b>
<b>EU</b>	<b>European Union</b>
<b>GB</b>	<b>Governing Board</b>
<b>HSM</b>	<b>Hardware Security Module</b>
<b>IoC</b>	<b>Indicator of Compromise</b>
<b>IPSec</b>	<b>Internet Protocol Security</b>
<b>ISAC</b>	<b>Information Sharing and Analysis Centre</b>
<b>JP</b>	<b>Joint Procurement</b>
<b>ML</b>	<b>Machine Learning</b>
<b>MS</b>	<b>Member State</b>
<b>OSI</b>	<b>Open Systems Interconnection</b>
<b>PKI</b>	<b>Public Key Infrastructure</b>
<b>SOC</b>	<b>Security Operation Centre</b>
<b>TCA</b>	<b>Total Cost of Acquisition</b>
<b>TESTA</b>	<b>Trans European Services for Telematics between Administrations</b>
<b>TLS</b>	<b>Transport Layer Security</b>
<b>VPN</b>	<b>Virtual Private Network</b>
<b>WP</b>	<b>Work Programme</b>