Call for expressions of interest to select entities that provide the necessary facilities to enlarge existing or host and operate new Cross-Border SOC Platforms/Cross-Border Cyber Hubs

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"[1]. 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[2] 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 programme (WP) for 2021-2022 included capacity-building actions for SOCs. The 2023 – 2024 WP aims at strengthening EU actions by supporting the creation of national SOCs, and networking them at European and EU level via cross-border SOCs and coordinating their activities to create a stronger SOC ecosystem, which will include local and regional, private and public security operational centres for both horizontal and vertical sectors.

As per the political agreement on the Cyber Solidarity Act[3] to be adopted and published in the Official Journal in autumn 2024, it is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the EU and to strengthen solidarity by enhancing Member States' and the EU's preparedness and ability to prevent and respond to significant, large-scale and large-scale-equivalent cybersecurity incidents.

The Cyber Solidarity Act envisages, as part of the European Cybersecurity Alert System, the establishment of a pan-European network of cyber hubs, to build and enhance coordinated detection and common situational awareness capabilities. It includes support for the development and consolidation of the national cyber hubs and the cross-border cyber hubs, also referred to as national SOCs/cross-border SOCs.

For the purpose of this call for expressions of interest, national SOCs could also be referred to as national cyber hubs and cross-border SOCs could be referred to as cross-border cyber hubs.

In this regard, under the EU's 'DIGITAL' funding program, EUR89 million are dedicated to "Security Operation Centres"[4] in the 2023-2024 cybersecurity work programme (WP). One of the key actions envisaged is enlarging existing cross-border SOC platforms or launching new ones. .

Those cross-border SOC platforms should enable and stimulate the exchange and fusion of large amounts of data on cybersecurity threats from multiple sources in a trusted environment. The platforms should also produce high quality, actionable intelligence for their participants through expert analysis and the use of state-of-the-art tools and infrastructures. This should serve to improve detection capabilities and ultimately the prevention of and response to cyber threats and incidents.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018
[2] SOCs potentially cover any entity or team tasked with detecting and acting on cyber threats
[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1332
[4] https://ec.europa.eu/newsroom/dae/redirection/document/100739

The purpose of this call for expressions of interest (CfEI) is to select entities in EU Member States and other eligible countries[5] willing to deploy and manage cross-border SOC platforms.

The selected consortia will engage in joint procurement with the ECCC to purchase the necessary tools, infrastructures and services to establish/enlarge the cross-border SOC platforms. For each joint procurement the EU will contribute up to 75% of the purchasing costs. The number of joint procurements to be conducted will depend on the number of successful applications selected following evaluation of this CfEI. The overall budget for procurement will be up to EUR 17 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 is successful at this call for expressions of interest. The EU will contribute up to 50% of eligible costs, such as staff costs or other eligible costs for setting up and running the cross-border platform, 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 cross-border platforms will come from the call for proposals on enlarging existing or launching new cross-border SOC platforms, having a total amount of EUR 5 million.

In the event of enlargement of an ongoing cross-border SOC, the new consortium will be composed of the coordinator of the ongoing grant plus the new entities that want to join the hosting consortium of the cross-border SOC.

The deployment of these cross-border 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 SOC entities at national level forming several cross-border SOC platforms, 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**.

2. Objectives of the cross-border platforms

The **general objective** of "**cross-border SOC platforms**" is to strengthen capacities to analyse, detect and prevent cyber threats and to support the production of high-quality intelligence on cyber threats, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention capabilities in a trusted environment. They should provide new additional capacity building upon and complementing existing SOCs and CSIRTs and other relevant actors.

The platforms should act as a central point allowing for broader pooling of relevant data and CTI, enable the spreading 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).

Cross-border SOC platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI, supporting the development of better performing data analytics, detection, and

[5] EEA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States

response tools, through the pooling of larger amounts of data, including new data generated internally by the consortia members.

The cross-border SOC platforms 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:
    - Within individual platforms. Participating actors in a cross-border platform must commit to sharing operationally relevant information between one another within the same consortium**.** 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 platforms. Conditions for exchanging information with other platforms are to be decided by each platform. The respective cooperation agreements should, in particular, specify information sharing principles and interoperability. The platforms should inform the Commission about the agreements concluded.

      As per the political agreement on the Cyber Solidarity Act to be adopted and published in the Official Journal in autumn 2024, ENISA is tasked with developing guidelines on the interoperability of cross-border cyber hubs. Against this background, the selected consortia will be required to collaborate with ENISA on the aspect of interoperability.
    - With relevant EU entities and networks. Platforms should provide an adequate level of information, as well as early warnings, to responsible networks and entities at EU level, in defined situations (such as in case of large scale cybersecurity incidents relevant information and early warnings must be provided to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs network) and subject to appropriate conditions, in order to support common situational awareness and effective crisis management and response.
- **Improving EU technological sovereignty.** Platforms should enhance the EU's cyber-threat knowledge base, support the development and improvement of the 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. Depending on the activities and conditions agreed by platforms, these services could be offered to the platform members, and, where possible, to the wider EU cybersecurity community, including EU industry and research and academia.

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

The purpose of this CfEI is to select entities that can provide the necessary facilities to host and operate cross-border platforms for pooling data on cybersecurity threat between several Member States. The call for expressions of interest will also build up the planning and design of necessary tools, infrastructures and services to be jointly purchased.

3.1 Selection of consortia

3.1.1 Selection of new consortia

This CfEI intends to select one or more multi-country consortia led by **public bodies from at least three Member States** that would come together to create cross-border SOC platforms. More specifically, it aims at selecting **consortia** composed of multiple **national SOCs** which will set up and manage cross-border SOC platforms. Members of a consortium must sign a consortium agreement among themselves outlining their various responsibilities, including the relevant information to be shared among the participants of the cross-border SOC platform.

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, etc.), or organisations that benefit from the services of the national SOC.

One or more of the national SOCs that participate in a consortium will take on the responsibility for the hosting of the cross-border SOC platform infrastructure. One of them will be designated as **'coordinator'** for the purpose of this CfEI. A cross-border SOC platform will be represented for legal purposes by the designated coordinator, or by the hosting consortium if it has legal personality. Hosting and usage agreements (HUAs) will be signed between the coordinators of the selected consortia, or the hosting consortium if it has legal personality, and the ECCC to decide on the operation and maintenance of the platforms' tools and infrastructure.

As this CfEI can be viewed as a first phase for new consortia, it may be necessary to evolve the platform(s) in a subsequent phase (further on called phase 2), with the aim of better achieving the objectives listed under Section 2 above. It should also be possible for additional national SOCs to join the consortia in subsequent phases, based on an agreement with the existing partners, with the aim of increasing and reinforcing the capabilities of the platforms (for more information, see Section 2).

In addition to participating partners, cross-border SOC platforms 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. 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 Enlargement of existing consortia

Under the 2021-2022 WP, the **first call for expressions of interest**[6] was launched to select entities in EU Member States and other eligible countries, willing to deploy and manage cross-border SOC platforms. The selected consortia have already engaged in joint procurement agreements with the ECCC to purchase the necessary tools, infrastructures and services to establish the cross-border SOC platforms.

As the CfEI launched under the 2021 - 2022 WP was viewed as a first phase for the selected consortia, 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, additional national SOCs could join the existing consortia based on an agreement with the existing partners, with the aim of increasing and reinforcing the capabilities of the platforms.

This CfEI intends to allow the existing consortia to apply for phase 2 of the project for the enlargement of the capabilities of the cross-border SOC platforms. If existing consortia decide to extend their operations to new members, they will sign an amendment to the consortium agreement outlining the enlarged structure of the consortium and their various responsibilities for the second phase of the project. 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

[6] https://cybersecurity-centre.europa.eu/system/files/2022-11/Call%20for%20Expression%20of%20Interest_Cross-border%20SOC%20platformsfinal.pdf

In response to this CfEI, applicants should submit a proposal that explains how the cross-border SOC platform will be established/enlarged, including the roles of the (new) participating partners. The application should explain in detail the goods and services that the participating national SOCs intend to jointly procure, via the coordinator, with the ECCC in order to establish/enlarge the cross-border SOC platform.

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 applicants' 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 establish/enlarge a cross-border SOC platform 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 cross-border SOC platform, which will be evaluated using the evaluation criteria established in the relevant call document under the Digital Europe Programme[7].

The procedure for establishing/enlarging a cross-border SOC platform with the support of funding provided under this call for expressions of interest and the relevant call for proposals[8] will be as follows:

1. This call for expressions of interest will lead to the selection of applicants intending to establish/enlarge a cross-border SOC platform.
2. For new consortia, each application must appoint a coordinator, with whom the ECCC will conclude a hosting and usage agreement if the application responding to the call for expressions of interest and the proposal submitted under the call for proposals are successful. The agreement can be signed with the hosting consortium if it has legal personality. 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 SOCs after joint procurement has been carried out. The coordinator will be a national SOC of one of the EU Member States participating in the consortium.

   For existing consortia, the coordinator will remain the one appointed in the first expression of interest, with whom the ECCC may conclude an amendment to the hosting and usage agreement and the joint procurement agreement. Before submitting the application, the coordinator is responsible for obtaining the approval of the enlargement by all the members of the hosting consortium.
3. Each selected coordinator/hosting consortium, if it has legal personality, will take part in joint procurement of goods and services with the ECCC. Several parallel joint procurement procedures may thus be launched. To this end, national SOCs of the other participating states in the consortium must transfer the required budget to the coordinator acting on their behalf. The ECCC and each coordinator/ hosting consortium, if it has legal personality, must sign a joint procurement agreement setting out the practicalities of the procurement procedure.

   The procurement of the tools, infrastructure and services needed for the enlargement of the existing consortia must comply with the conditions and requirements related to the purchase of new goods and services set out in the tender specifications for the first phase of the joint procurement. In accordance with the provisions of the Financial Regulation, the ECCC and the consortium will proceed with a procurement procedure and the award of a new contract for the additional tools, infrastructures and services needed for the enlargement.

   The joint procurement agreement between ECCC and the coordinator of the hosting consortium may need to be amended upon ECCC request to agree on the practicalities of the procurement procedure for the additional tools, infrastructure and services required for the enlargement of

[7] See section DIGITAL-ECCC-2024-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)
[8] See section DIGITAL-ECCC-2024-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)

the cross-border SOC platform. The new participants in the consortium must transfer the required budget to the coordinator acting on their behalf.

4. The consortium has also to apply for a complementary grant, to cover eligible costs, such as the cost of setting up and running the cross-border SOC platform. To be eligible for such a grant, applicants must submit the proposal for a grant in response to the relevant call for proposals opened on 4 July 2024, following the procedure established for that purpose.

   By submitting an application in response to the CfEI, all participating partners in the consortium 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. 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.

   In the event of enlargement of an ongoing cross-border SOC platform, the new consortium will be composed of the coordinator of the ongoing grant plus the new entities that want to join the cross-border SOC. The new grant will work seamlessly with the ongoing one.

Consortia willing to host and manage cross-border SOC platforms 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 17 million for all cross-border SOC platforms. The EU contribution would cover up to 75% of the purchasing costs of the tools, infrastructures and services. The remaining procurement costs would be covered by Member States participating in each cross-border SOC platform. The EU contribution can only be used for jointly purchased goods and services.

In addition, consortia have to apply for a grant to cover other costs through a separate call for proposals[9]. The EU funding rate for such a grant is maximum 50%.

Successful consortia for 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 establish/enlarge those platforms.

To that end, the ECCC will conclude hosting and usage agreements only with the consortia that are selected following this CfEI and that have been awarded a grant under the call DIGITAL-ECCC-2024-CYBER-07-SOCPLAT. This condition is cumulative.

Joint procurement(s)

The financial rules of the ECCC, adopted through DECISION No GB/2023/1[10] 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 establish cross-border SOC platforms will be carried out by the ECCC (or the Commission acting on behalf of the ECCC until the ECCC becomes financially autonomous) in accordance with the ECCC financial rules and using the ECCC procedural provisions. The ECCC will jointly acquire, with each hosting consortium/coordinator representing each cross-border SOC platform selected further to the CfEI, relevant components of a cross-border SOC platform and will co-own them with the participating Member States (or their consortium representatives) in that consortium that provide a share of the funding. Share of ownership will correspond to share of the funding provided.

If the hosting consortium does not have legal personality, the coordinator will represent the consortium and be authorised to sign the hosting and usage agreement, the joint procurement agreement and subsequent

[9] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2024/call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf

[10] https://cybersecurity-centre.europa.eu/system/files/2023-04/ECCC%20Decision%20No%201%20GB%202023_ECCC%20Financial%20Rules.pdf

amendments to both agreements, if needed, on behalf of all national SOCs participating in the consortium. Each consortium must ensure that national SOCs that provide a share of the funding have agreed in advance to transfer their individual share of at least 25 % of the overall estimated procurement costs not covered by the EU contribution to the coordinator, so that the coordinator can engage in joint procurement with the ECCC[11]. Evidence of this commitment must be provided as part of the application in response to the CfEI.

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

As part of their application, applicants for new cross–border SOC platforms 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.

In the event of enlargement of existing cross–border SOC platforms, applicants are required to submit, as part of their application, a revised version of the hosting and usage elements specific to the application.

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, dedicate 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. 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 2023 – 2024[12] apply in this regard.

3.3 Applications for complementary grants

Separately from this call for expressions of interest, the selected consortia have to apply to be supported through grants awarded further to the call for grant proposals on SOCs mentioned above. Procedures are described in the relevant call document[13].

Examples of specific activities which may be supported under the grant are provided in the text of that call for grant proposals on enlarging existing or launching new cross-border SOC platforms[14], whereas the eligible costs are defined in the general model grant agreement of the Digital Europe Programme.[15] Eligible costs may include

---

[11] It is for the MS participating in the cross-border SOC to agree among themselves as to the respective contributions to the remaining the acquisition costs, to transfer this to the coordinator, and to empower the coordinator to act on their behalf for the purpose of a joint procurement.

[12] https://ec.europa.eu/newsroom/dae/redirection/document/100739

[13] See section DIGITAL-ECCC-2024-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)

[14] See section DIGITAL-ECCC-2024-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)

[15] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/agr-contr/mga_dep_en.pdf

the costs for maintenance or recurrent licences required for running the cross-border SOC and which cannot be purchased as part of the joint procurement(s).

Grants may cover up to 50% of eligible costs of the participating national SOCs for setting up/enlarging a cross-border SOC and running it.

Applications to receive such a grant must be submitted separately through the grants Funding&Tenders Portal.[16]

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

In the event of enlargement of an ongoing cross-border SOC platform, the new consortium will be composed of the coordinator of the ongoing grant plus the new entities that want to join the hosting consortium of the cross-border SOC and the new grant will work in close cooperation with the ongoing one.

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 participants" must provide administrative **details about the participants** to the cross-border SOC platform initiative presented, including contact details and legal representatives. It should set out the role of each participant, their competencies and their contribution to the project.

In the case of enlargement of an on-going SOC platform, the **Annex "Information on the participants"** must provide administrative details about the new participants to the cross-border SOC platform initiative presented.

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 setting up/enlarging the cross-border platforms 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 separate application for grants. Applicant 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.

[16] EU Funding & Tenders Portal | EU Funding & Tenders Portal (europa.eu)

4.2. Key features of cross-border SOC platforms[17]

This section describes the main features of the national SOC platforms / national cyber hubs, as background information when completing the submission form.

If several submissions to the CfEI are received and selected, an appropriate level of synergies and collaboration will be required between them and the existing cross-border SOC platforms. In particular, the cross-border SOC platforms should adopt consistent and interoperable approaches and standards, in order to allow for possible exchanges of information among them at a later stage, as appropriate. As per the political agreement on the Cyber Solidarity Act to be adopted and published in the Official Journal in autumn 2024, the cross-border SOC platforms should enter into cooperation agreements with other cross-border SOC platforms which should, in particular, specify information sharing principles and interoperability. To support such interoperability, ENISA is required to issue interoperability guidelines, developed in particular with taking into account the functioning of established Cross-Border SOCs/Cyber Hubs. 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 governance.** This section should explain the overall vision for the platform, and how it will be governed in terms of decision structures. It should demonstrate how this would lead to an increased data sharing and better detection capability for cyber threats. The governance framework should be designed to foster engagement and trust among participants. Proposals should also consider how the proposed platforms will help expand the EU's cyber -threat knowledge base and make the EU more technologically independent.
    - **Minimum condition for the expression of interest.** As set out above, a cross-border SOC platform should be a platform managed by national SOCs (public entities acting as hubs) for exchanging data on cybersecurity threats and incidents with public and private actors. 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 participation in the platform should be outlined in the submission. While the platforms will be led by public entities, a concrete engagement from the private sector, or at least a clear strategy for engaging 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, with well-defined and appropriate enrolment conditions and vetting procedures. It should address data sharing (see below), security and access rights, vetting and participation conditions. If several platforms are selected, a working group to share best practices will be created.
- **Interoperability within and between cross-border SOC platforms:**
    - **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.** If several platforms are selected, they will be required to agree on a single common data format and taxonomy and on a common data structure, in order to enable interoperability and potential data sharing across platforms 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.

[17] In the framework of the ECCC Governing Board, Commission services and Member States representatives developed a concept paper on "Future EU actions on cyber threat detection and sharing". This concept paper notably identifies key dimensions (governance, incentives, interoperability, infrastructure) that should inspire the establishment of the cross-border SOC platforms.

- **Data management (level of data sharing, conditions and incentives and legal aspects)**
    - **Minimum condition for the expression of interest.** Consortia members should demonstrate the willingness to share as much information as possible with the due level of speed and quality. Consortium members should define and commit to a significant level of data sharing within their platform. 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 governance framework referred to under point 1 above, clear and appropriate rules of engagement should be drawn up so as to incentivise the various participants to join and share information. This should include detailed terms of reference, covering aspects such as data sharing (ownership, control, compliance, management), security and access rights. Engagement should be based on a mutually agreed approach to reward sharing of data and information and assess data quality, which makes it easy to participate and creates a sense of fairness to all other participants. For instance, this could be based on a set of indicators to measure stakeholder participation in terms of the amount of information shared, quality and type of information, and a set of corresponding rewards (e.g., access to more detailed info). If several platforms are selected, they will be encouraged to join a working group to share best practices. Prospective consortia are invited to include such task in the grant part of their proposal.
- **Contribution to EU-level situational awareness:**
    - **Minimum condition for the expression of interest.** The platforms should contribute to the strengthening of the EU's collective situational awareness and detection capabilities. For this, they should provide an adequate level of information and early warnings to responsible networks and entities at EU level, in defined situations (such as in case of large scale cybersecurity incidents) and subject to appropriate conditions, in order to support common situational awareness and effective crisis management and response. To specify situations and conditions, they should engage with other platforms at the EU level.
- **Highly secure infrastructure and state-of-the-art technologies and tools:**
    - **Minimum condition for the expression of interest.** Candidate consortia 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 EU technological independence.
    - **Objective to be achieved during tender preparation phase.** If several platforms are selected, all selected consortia will be required to work together on the preparation of the draft tender specifications for the procurement procedures. For this, they will be encouraged to consider a common approach, taking the common blueprint architecture described in Annex 5 as a starting point. This effort will aim at identifying common equipment, tools, etc. to be purchased through the joint procurement actions, where possible (see Section **Errore. L'origine riferimento non è stata trovata.**). As regards security and secure communication channels, consortia should commit to meet 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 EU detection capabilities:**
    - **Minimum conditions for the expression of interest.** Candidate consortia 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 the conditions agreed on by platforms, these services could be offered to the platform members, and where possible, to the wider EU cybersecurity community, including EU 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.** If several platforms are selected, they will be encouraged to work together to identify synergies between other services and activities provided by individual platforms. 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 cross-border SOC platforms 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 cross-border SOC platform must be represented for legal purposes, including for submitting the expression of interest, by a member of the corresponding hosting consortium acting as a coordinator, or by the hosting consortium if it has legal personality. The coordinator must be a public body of a Member State, which will represent a consortium of participants that has agreed to contribute to the acquisition and operation of the cross-border SOC platform.

2 If the hosting consortium does not have legal personality, the coordinator must present the proposal on behalf of the consortium.

3 For new cross-border SOC platforms, the consortium must involve public bodies designated as national SOCs from at least three Member States in a first phase, with a possibility of more joining in later phases.

4 The coordinator and the other participating partners belonging to the consortium must have legal personality.

5 The coordinator may envisage hosting and managing the cross-border SOC platform wholly or partially.

6 The coordinator must be empowered to participate in a joint procurement action with the ECCC and formally represent the public bodies of the participating Member State. Each Member State participating in a consortium must provide a commitment to transfer the required acquisition costs to the coordinator so that the coordinator may engage in joint procurement with the ECCC on their behalf. For this purpose, each application must contain copies of Annex 4 ('Commitment and mandate letter') completed by each entity participating in the consortium.

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

The coordinator of the consortium presenting an expression of interest will act as intermediary for all communications between the Commission, the ECCC and the participating partners. However, partners are jointly responsible for implementing the actions described in the expression of interest, if finally retained, and must make the appropriate internal arrangements.

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

Award criteria for the expression of interest

Criterion	Score
General concept and governance: • Quality of the vision, development plans and capability of the consortium to set up/enlarge and manage the cross-border SOC platform and to create a trusted environment stimulating the active participation and sharing of its consortium members • Added value with relation to existing structures • Contribution to the EU's technological independence (e.g., use of EU made solutions, EU sourced data) • Sustainability of collaboration in the longer term • Feasibility and credibility of the presented approach	0-20 points
Feasibility and quality of the interoperability: • Use of common data format and taxonomy • Quality of the proposed approach for interoperability and trusted interaction and data exchange between the partners of the cross-border SOC platform • Use of international recognised standards, protocols, best practices and guidelines to guarantee interoperability with other cross-border SOC platforms, and commitment to cross-platform cooperation and/or integration plans	0-15 points
Highly secure infrastructure and state-of-the-art technologies and tools • Quality and effectiveness of the proposed plan for the readiness of the site to host the system • Security of the infrastructure • Use of most advanced technologies and tools based on market review • Compliance with the system specifications set out in this CfEI • Quality and pertinence of the current and proposed hosting facility's physical and IT infrastructure, its security, and its connectivity • 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	0-15 points

Data management • Quality and effectiveness of proposed plan for data management (e.g., access rights, ownership, control) • Commitment to share information among them by members of the platforms • Mechanisms to encourage data sharing by all contributors to the platforms • Approach to legal aspects (e.g., compliance with legislation, anonymisation, etc.)	0-15 points
Contribution to EU-level situational awareness • 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).	0-15 points
Provision of other services and activities to strengthen EU detection capabilities • Quality and effectiveness of the proposed services and activities to contribute to EU capabilities • Links with existing and future relevant EU-funded initiatives and projects	0-10 points
Goods and services to be procured and total cost of acquisition (TCA) • Suitability of proposed goods and services to be jointly procured to achieve the objectives of the cross-border platform • Clarity and effectiveness of the estimated TCA of the cross-border SOC platform, focusing on the total cost of what will be needed to be procured under the joint procurement(s) to run the platform	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 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 form the basis for further assessment.
- Consensus meetings. After carrying out their individual assessment of the expressions of interest, 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 assessment. 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 the 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 draw up a final ranking list based on the list proposed by the panel. The Executive Director may suggest to the authorising authority (i.e., the European Commission before the ECCC becomes financially autonomous, and the ECCC Governing Board afterwards), to deviate from the ranking proposed by the panel with a justification.

This final ranking list will consist of:

1. A main list with the expressions of interest to be selected as proposed by the experts complemented by any suggestion for deviation from this list as proposed by the Executive Director.
2. A reserve list, with expressions of interest that have passed the assessment thresholds. Those in the reserve list might be offered the possibility to become selected and thus, conclude a hosting and usage agreement, in case for whatever reason a hosting and usage agreement cannot be concluded with a higher ranked expression of interest or if additional funds become available.

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.

The Executive Director will submit the final ranking list to the authorising authority with a proposal for selection of applications for its approval. Moreover, the Executive Director will in due course inform the ECCC Governing Board and the DEP program committee.

The authorising authority will make the final selection of applicants, who will be invited to conclude a hosting and usage agreement with the ECCC.

After the decision of the authorising authority, 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 expressions of interest.

The ECCC will subsequently invite the selected applicants to the next stages for the signature of the hosting and usage agreement (or an amendment to the hosting and usage agreement for the existing cross-border SOC platforms, if applicable), and the preparation of the joint procurement(s) of goods and services for cross-border SOC platforms, including the signing of a joint procurement agreement (or an amendment to the joint procurement agreement for the existing cross-border SOC platforms, if applicable). 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 authorising authority before they are signed by the respective parties.

6.3. Communication

This 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: CNECT-ECCC-DEP@ec.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 those submitting expressions of interest, 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 cal.

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 CNECT-ECCC-DEP@ec.europa.eu.

All communication regarding an expression of interest will take place with the coordinator only, unless there are specific reasons to do otherwise, in which case the consortium coordinator must be put in copy.

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 coordinator.

7. Tentative timetable

- 21 January 2025: deadline to submit expressions of interest to set up cross-border SOC platforms and request for complementary grants under call DIGITAL-ECCC-2024-CYBER-07-SOCPLAT. **This deadline is definite, not tentative.**
- May 2025: finalisation of assessment of expressions of interest and grant application
- Q3 2025: signing of joint procurement/hosting and usage agreement
- Q 4 2025: work with experts to draft technical specifications for joint procurement call(s) for tender
- Q1 2026: publication of joint procurement call(s) for tender by ECCC and cross-border SOC platforms
- Q2 2026: signing of procurement contract with selected contractors

8. Procedure for the submission of expressions of interest

Expressions of interest must be submitted before the call deadline **21 January 2025 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 be submitted separately by responding to the call for proposals on the Funding and Tenders portal[18].

Contact point for any questions is CNECT-ECCC-DEP@ec.europa.eu.

You have specific rights regarding the 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.

[18] EU Funding & Tenders Portal | EU Funding & Tenders Portal (europa.eu)

Annexes

The annexes to this call for expressions of interest are:

- Annex 1A: **Information on the participants to new cross-border SOCs.**
- Annex 1B: **Information on the participants to the enlargement of existing cross-border SOCs**.
- Annex 2: I**nformation on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment and mandate letter**
- Annex 5: **Blue-print architecture**

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

- Annex 1A: **Information on the participants to new cross-border SOCs.** Applicant must provide administrative **details of the participants** to the new cross-border SOC platform initiative presented, including contact details and legal representatives. It should present the role of each participant, their competencies and their contribution to the project.
- Annex 1B: **Information on the participants to the enlargement of existing cross-border SOCs**. Applicants must provide **details of the new participants** to the existing cross-border SOC platform, including contact details and legal representatives. It should present the role of each participant, their competences and their contribution to the project.
- Annex 2: I**nformation on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment and mandate letter**

List of abbreviations

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