Call for Expression of Interest to select entities that provide the necessary facilities to host and operate cross-border platforms for pooling data on cybersecurity threats between several Member States ('Cross-border SOC platforms')

1. Introduction

In a context of accelerated digitisation as well as growing number and impact of cybersecurity incidents, the European Commission (EC) adopted the "EU Cybersecurity Strategy for the Digital Decade"[1] in December 2020. Among other objectives, the Cybersecurity Strategy aims to improve capacities and cooperation to detect cyber threats, before they can cause large-scale damage, in view to detect more threats and do so much faster.

The Russian invasion of Ukraine further underlines and reinforces the need to urgently step up cybersecurity capabilities at national and at Union level, including by intensifying the exchange of information and improving detection of cybersecurity threats in order to promote better situational awareness and inform preventive and response actions.

The EU Cybersecurity Strategy proposes to build, strengthen, and interconnect, across the European Union (EU), Security Operation Centres (SOCs) and Cyber Threat Intelligence (CTI) capabilities (monitoring, detection and analysis), with the aim to support 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 Security Operation Centres (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, under the EU funding program DIGITAL, €110 million are dedicated in the cybersecurity work programme (WP) 2021-2022 to "Capacity Building of Security Operation Centres"[3]. One of the key envisaged actions is the setting up of '***cross-border platforms for pooling data on cybersecurity threats*** *between several Member States'.*

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, and 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 prevention and response to cyber threats and incidents.

The purpose of this Call for Expression of Interest (CfEI) is to select entities in EU Member States and other eligible countries[4], 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 and infrastructures to establish 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 needs identified under this CfEI. The budget for procurement will consist of up to €30 million.

[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/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf

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

Separately, a platform could receive a grant to complement the joint procurement(s). The related grant would be awarded, if the relevant requirements in the separate call for proposals are met. It would cover up to 50% of eligible costs, such as staff costs or other eligible costs for setting up and running the cross-border platform, with the exception of those tools and infrastructures 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 Security Operation Centres (SOCs), having a total amount of €72,5 million.

The deployment of these cross-border platforms is a pivotal component in a wider strategy and set of actions aimed at stepping up monitoring and detection capabilities and improving situational awareness at national, cross-border and EU level, and at paving the way for building a **collaborative, interoperable and sustainable pan-European infrastructure.** The infrastructure will link SOCs entities at national level forming several cross-border SOC platforms, that will be able to build up shared capacities and exchange information among themselves. Such platforms would together constitute a pan-European 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** as well as specific conditions aimed at ensuring 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 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 advanced data analytic tools (including for example Artificial Intelligence (AI) / 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 Union collective situational awareness and 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 is to be decided by each platform.
    - 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 cross-border incidents) and subject to appropriate conditions, in order to support common situational awareness and effective crisis management and response.
- **Improving EU technological sovereignty**: the platforms should enhance the EU's cyber-threat knowledge base, supporting the development of EU tools and their improvement, and help creating and structuring 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 several data lakes, the provision of cyber range services, and/or training of cybersecurity analysts. Depending on the activities and the 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 Expression of Interest (CfEI)

The purpose of this CfEI is to to select entities that provide the necessary facilities to host and operate cross-border platforms for pooling data on cybersecurity threat between several Member States.

3.1 Selection of consortia

This CfEI intends to select one or more multi-country consortia led by **competent authorities from at least 3 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.

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.

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 shall be designated as **'coordinator'** for the

purpose of this CfEI. Hosting and usage agreements will be signed between the coordinators of the selected consortia 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, 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. 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). Participation from defence entities should be allowed.

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.

3.2 Overview of the process

Applicants should submit a proposal to this CfEI that explains how the cross-border SOC platform will be established, including the roles of the participating partners. The application should explain in detail the goods and services which the participating National SOCs intend to jointly procure, via the coordinator, with the ECCC in order to establish 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 a cross-border SOC platform will be evaluated using the evaluation criteria established in this document.

Separately, applicants may 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[5]

The procedure for establishing a cross-border SOC platform with the support of funding provided under this Call for Expressions of Interest will be as follows:

1. This Call for Expressions of Interest will select applicants intending to establish a cross-border SOC platform.
2. Each application shall appoint a coordinator, with whom the ECCC will conclude a hosting and usage agreement. This agreement will set out practical arrangements for managing the hosting and usage of the tools and infrastructures 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.
3. Each selected coordinator will take part in joint procurement of goods and services with the ECCC. Several parallel joint procurements may thus be launched. To this end, National SOCs of the other participating states

[5] See section DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) in the call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)

in the consortium must transfer the required budget to the coordinator acting on their behalf. The ECCC and each coordinator shall sign a joint procurement agreement setting out the practicalities of the procurement procedure.

4. Separately, the participating partners in each selected consortium may apply for a complementary grant, for covering eligible costs, such as setting up and running the cross-border SOC platform. In order to be eligible to receive such a grant, applicants must submit the proposal for a grant in the relevant call for grants opened on 15 November 2022, following the procedure established for that purpose.

   By submitting an application to the CfEI all participating partners in the consortium provide their prior acceptance with the terms and conditions set in the model hosting and usage agreement. The model hosting and usage agreement is found in Annex 3 of 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.

Consortia willing to host and manage cross-border SOC platforms will be selected through this Call for Expression of Interest. Successful consortia will engage in joint procurement with the ECCC to purchase the necessary tools and infrastructures to establish those platforms.

For the joint procurement(s), the EU financial contribution is estimated at a maximum of €30 million for all cross-border SOC platforms. The EU contribution would cover up to 75% of the purchasing costs of the tools and infrastructures. 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 can apply for a grant to cover other costs through a separate call for grants[6]. The EU funding rate for such a grant is 50%.

Joint Procurement(s)

The financial rules of the ECCC, soon to be adopted, shall set out the conditions under which the ECCC may engage in procurement, including joint procurement with the Member States.

The joint procurement(s) for tools and infrastructures 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 shall jointly acquire, with each coordinator representing each cross-border SOC platform selected further to the CfEI, relevant components of a cross-border SOC platform and shall co-own them with the participating Member States (or their Consortium representatives) in that consortium who provide a share of the funding. Share of ownership shall correspond to share of the funding provided.

The coordinator shall represent the consortium and be authorised to sign both the hosting and usage agreement and the joint procurement agreement on behalf of all National SOCs participating in the consortium. Each consortium must ensure that National SOCs who provide a share of the funding have agreed in advance to transfer their individual share of the at least 25 % overall estimated procurement costs not covered by the

[6] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2022-cyber-03-soc

Union contribution to the coordinator, so that the coordinator can engage in joint procurement with the ECCC[7]. Evidence of this commitment must be provided as part of the application to the CfEI.

By submitting the application, applicants provide their prior acceptance with the terms and conditions set in the model hosting and usage agreement. The model hosting and usage agreement is found in Annex 3 of this CfEI. **As part of their application, applicants are required to supplement the model hosting and usage agreement by completing that part of the agreement which 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.**

A technical group composed of experts from the EU Member States has been set up to support the process and in particular, to help identify the main types of goods and services that would need to be jointly procured and to discuss a common, high-level blueprint architecture, see Annex 5.

Typical examples of goods and services to be procured, as identified so far by the technical group, 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 the 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)**. This means that **the vendors of the goods and services to be procured should be EU controlled entities**, or EEA controlled entities[8]**.**

3.3 Possibility to apply for complementary grants

[7] 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.

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

Separately from this Call for Expression of Interest, the selected consortia may apply to be supported through grants awarded further to the call for grant proposals on SOCs mentioned above. Modalities are described in the relevant call document[9].

Examples of specific activities which may be supported under the grant are provided in the text of that call for grant proposals on SOCs[10], whereas the eligible costs are defined in the general model grant agreement of the Digital Europe Programme.[11] Eligible costs may include 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 a cross-border SOC and for running it.

Applications to receive such a grant should be submitted separately through the grants portal.[12]

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

4. Content of the applications

4.1. Participants must fill 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 present the role of each participant, their competences and their contribution to the project.

> N.B: *Addition of new participants* - In addition, as part of the reply to the CfEI, participants must provide a **formal statement indicating the conditions for including additional participating Member States or their official representatives in subsequent phases of the project.**

2) The second Annex ("Information on the expression of interest") relates to the Joint procurement(s) and should be filled 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 indicated points.
>
> - 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 the cross-border platforms and their projected costs.**
>
> - Information about existing infrastructures and other resources offered by those replying to the CfEI.

[9] See section DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) in the call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)

[10] See section DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) in the call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)

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

[12] Funding & tenders (europa.eu)

- A short description of the complementarity with any separate application for grants, in case such a separate application is planned: provide a summary of the grant part of the project and explain the link between the procurement and the grant parts, elaborating on how one complements the other and which aspects and costs they cover respectively.

4.2. Key features of cross-border SOC platforms[13]

This section aims at informing the preparation of the submission form, by describing the main features of the cross-border platforms.

In case several submissions to the CfEI are received and selected, an appropriate level of synergies and collaboration between them will be required. 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. They should be congruent with the high-level, blueprint architecture discussed by the group of technical experts (see 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 to what extent the proposed platforms will contribute to increase the EU's cyber threat knowledge base and technological independence.
    - **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 minimum 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, 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. In case several platforms are selected, a working group to share best practices will be created.
- **Interoperability within and between cross-border SOC platforms:**

[13] 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.

- **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 MISP and of the relevant state of the art IT tools is strongly recommended.
- **Objective to be achieved during deployment phase:** In case 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.

- **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 defined so as to incentivise the various participants to join and share information. This should include detailed terms of reference, which address 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 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 the level of participation of stakeholders in term of amount of information shared, quality and type of information, and a set of corresponding rewards (e.g., access to more detailed info). In case 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 Union collective situational awareness and detection capabilities. For this, they should provide an adequate level of information to responsible networks and entities at EU level, in defined situations (such as in case of major cross-border 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 and 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 a 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. For what concerns secure communications, to ensure future interoperability across the different platforms, all submissions 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:** in case several platforms are selected, all selected consortia will be required to work together on the preparation of the draft tender specifications for the procurement(s). In this context, they will be encouraged to consider a common approach, taking the common blueprint architecture developed by the group of MS technical experts 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, as much as possible (see Section **Error! Reference source not found.**). As regards s ecurity and secure communication channels, consortia should commit to meet very high standards (if necessary, in a gradual way). The possibility to use and build upon existing building blocks (such as MeliCERTes) as well as elements of the EU-funded cloud-based infrastructure for data spaces that is currently under development should also be explored.

- **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 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:** In case several platforms are selected, they will be encouraged to work together to identify synergies between other services and activities provided by individual platforms. In this context, they could for instance explore the possibility of creating one or several data lakes (cf. section 2 above).

5. Eligibility and award criteria

In order to be eligible, the expression of interest for the joint procurement(s) must satisfy simultaneously the following conditions:

Expression of interest

1. The **expression of interest** must be submitted in due time as stated in Section 7, following the procedure detailed in Section 8.
2. The **expression of interest** must be complete 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.

MS authority submitting the expression of interest

1 The coordinating entity submitting the expression of interest (called 'coordinator' in what follows) must be a public authority of a MS, which will represent a consortium of participants that has agreed to contribute to the acquisition and operation of the cross-border SOC platform.

2 The coordinator should present the proposal on behalf of the consortium.

3 The consortium must involve public authorities from at least 3 MSs 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 foresee to host and manage 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 authorities of the participating MS. Each MS participating in a consortium must provide a commitment to transfer the required acquisition costs to the coordinator so that the coordinator may engage in a joint procurement action 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 an 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, making appropriate internal arrangements.

Award criteria: Proposals shall 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 and manage the cross-border SOC platform and to create a trusted environment stimulating the active participation and sharing of its Consortium members.	0-20 points

• 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 on the longer term • Feasibility and credibility of the presented approach	
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 for 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 defined 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	0-15 points

• 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).	
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 the implementation of the assessment of the received expressions of interest. It shall 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 EC staff acting on behalf of the ECCC 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 on the basis of the assessment criteria described in Section 5, getting a score for each criterion, with explanatory comments. These scores and comments will be captured in individual reports form the basis of the further assessment.
- Consensus meetings. After carrying out their individual assessment of the expressions of interest, those involved in the assessment shall convene in a consensus meeting, to agree on a common position, including comments and scores and prepare a consensus report.

- Panel review. 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 marks or revised comments and resolve cases where there are different views. The panel will prepare an assessment report, in which it establishes its final ranking list and scores according to the award criteria provided in Section 5. Only expressions of interest above threshold will be ranked by the review panel according to the award criteria 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*". When these scores are equal, priority will be based on the scores for the award criterion "*data management*". When 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, in case 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 elaborate a final ranking list based on the list proposed by the panel. The Executive Director may suggest to the authorising authority (i.e., the EC before the ECCC is financially autonomous, and the ECCC GB afterwards), to deviate from the ranking proposed by the panel with a justification.

This final ranking list shall 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 whichever reason a hosting and usage agreement cannot be established with a higher ranked expression of interest or additional funds become available.

In addition, the ECCC will prepare 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 inform in due time the ECCC GB and the DEP program committee.

The authorising authority will make the final selection of applications, which will be invited to establish 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 invite the selected expressions of interest 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 cross-border SOC platforms, including the signature of a joint procurement agreement, but the invitation is not a commitment that

the ECCC will launch the procurement procedures. The hosting and usage agreement, and the joint procurement agreement, shall be approved by the authorising authority before their signature by the respective parties.

6.3. Communication

The information contained in the present 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 present call.

All enquiries must be made by e-mail only to: CNECT-ECCC-GB@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 those submitting expressions of interest, or affiliated entity(ies), an action or specific activities.

No individual replies to questions will be sent but all questions together with the answers and other important notices will be published (FAQ in EN) at regular intervals on the website under the relevant call: https://cybersecurity-centre.europa.eu/index_en

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 modification to the expressions of interest is allowed 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 those submitting expressions of interest for this purpose during the assessment process. This is generally done by e-mail. It is entirely the responsibility of those submitting expressions of interest 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-GB@ec.europa.eu.

All communication regarding an expression of interest will be done with the coordinator only, unless there are specific reasons to do otherwise, where the consortium coordinator should be in copy.

Those submitting expressions of interest will be informed in writing about the results of the selection process. Unsuccessful ones 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

- 15 February 2023: deadline to submit expressions of interest to set up cross-border SOC platforms and request for complementary grants under call DIGITAL-ECCC-2022-CYBER-03-SOC
- Mid-March 2023: finalisation of assessment of expressions of interest and grant application.
- Q2 2023: signature joint procurement/hosting and usage agreement.
- Q 2 2023: work with experts to draft technical specs of joint procurement(s) call for tender.
- Q2 2023: publication of joint procurement(s) call for tender by ECCC and cross-border SOC platforms.

- 2nd half 2023: signature of procurement contract with selected vendors.

8. Procedure for the submission of expressions of interest

Expressions of Interest must follow this submission procedure:

- Expressions of Interest must be sent electronically no later than the DATE+TIME Brussels time at the functional mailbox CNECT-ECCC-GB@ec.europa.eu.
- Expressions of Interest must be submitted using the Submission Form available in Annex 1. Section 4 provides information on how to fill the Submission Form.
- Expressions of interest must be submitted in the English language, in the correct form, duly completed, and dated.

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

Annexes

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

- Annex 1: **Information on the participants.** Applicant must provide administrative **details about the participants** to the cross-border SOC platform initiative presented, 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**

Expressions of Interest must be sent electronically no later than the DATE+TIME Brussels time at the functional mailbox CNECT-ECCC-GB@ec.europa.eu.

Annex 1. Information on the participants

1.1. Participant No 1 – Coordinator

1.1.1 IDENTITY OF THE PARTICIPANT
Official name in full:
Acronym: (if applicable)
Official legal form:
Legal personality[14]:
Place of establishment or registration: (Address and country)
Entity registration number: (Not applicable if the participant is a public-sector body.)
VAT number (if applicable):

The legal details are attached in the Legal Entity Form[15] to be provided as annex. Any changes in the legal entity form must be notified in writing to the Executive Director.

1.1.2 CONTACT DETAILS
Street address:
Postcode:
City:

[14] Legal personality is understood as participant's capacity to sign contracts and constitute a party in court proceedings under the applicable national legislation.

[15] http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal-entities_en.cfm

Region (if applicable):	
Country:	
Telephone:	Mobile:
Fax:	
E-mail address:	
Website:	

Any change in the addresses, phone numbers, fax numbers or e-mail, must be notified in writing to the Executive Director. The Executive Director will not be held responsible in the event that it cannot contact a participant**.**

1.1.3 CONTACT PERSON RESPONSIBLE FOR THE EXPRESSION OF INTEREST	
Family name:	First Name:
Position/Function:	
Telephone:	Mobile:
Fax:	
E-mail address:	
1.1.4 LEGAL REPRESENTATIVE	
Family name:	First Name:
Position/Function/Mandate:	
Telephone:	Mobile:
Fax:	

E-mail address:

1.2. Participant No 2 (if applicable, repeat this part as often as is required to include all participants)

1.2.1 IDENTITY OF THE PARTICIPANT
Official name in full:
Acronym: (if applicable)
Official legal form:
Legal personality[16]:
Place of establishment or registration: (Address and country)
Entity registration number: (Not applicable if the participant is a public-sector body.)
VAT number (if applicable):

The legal details are attached in the Legal Entity Form[17] to be provided as annex. Any changes in the legal entity form must be notified in writing to the Executive Director.

1.2.2 CONTACT DETAILS

[16] Legal personality is understood as participant's capacity to sign contracts and constitute a party in court proceedings under the applicable national legislation.

[17] http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal-entities_en.cfm

Street address:	
Postcode:	
City:	
Region (if applicable):	
Country:	
Telephone:	Mobile:
Fax:	
E-mail address:	
Website:	

Any change in the addresses, phone numbers, fax numbers or e-mail, must be notified in writing to the Executive Director. The Executive Director will not be held responsible in the event that it cannot contact a participant**.**

1.2.3 CONTACT PERSON RESPONSIBLE FOR THE EXPRESSION OF INTEREST	
Family name:	First Name:
Position/Function:	
Telephone:	Mobile:
Fax:	
E-mail address:	

Annex 2. Submission form for the expression of interest

IMPORTANT NOTICE

Those submitting expressions of interest must use this template for their submission (designed to highlight important aspects and facilitate the assessment against the award criteria).

***Character** and **page limits**:*

1. *page limit: 90 pages*
2. *minimum font size — Arial 8 points*
3. *page size: A4*
4. *margins (top, bottom, left and right): at least 15 mm (not including headers & footers).*

Please abide by the formatting rules. They are not a target! Keep your text as concise as possible. Do not use hyperlinks to show information that is an essential part of your project.

Please include in the header (top left) of each page the reference acronym of the expression of interest.

Before filling in this form, please read carefully the relevant CfEI, and any other reference documents related to this call available on our site: https://cybersecurity-centre.europa.eu/index_en

Please make sure that your expression of interest:

a) is submitted on the correct form, completed in full and dated;

b) is signed by the person authorised to enter into legally binding commitments on behalf of the participant;

c) meets the submission arrangements set out in the CfEI;

d) is submitted by the deadline.

⚠ *Paragraphs in italics are intended as explanatory guidance for the submission and shall be deleted before bidding.*

⚠ *Don't forget to delete this box and explanatory text in italics.*

PROGRAMME CONCERNED
XXX
REFERENCE NUMBER OF THE CALL OF EXPRESSION OF INTEREST
XXX
SUMMARY OF THE EXPRESSION OF INTEREST
Reference name of the expression of interest:
Reference acronym of the expression of interest:
Identity of the coordinator:
Consortium: *YES/NO*
Summary of the expression of interest: (*in EN, max 1000 words)*
Conditions for accepting additional participating partners if selected. Please include also the indicative amounts of the contribution of the additional participating partners:

2. Information on the expression of interest

*Please provide a detailed description of the project, its **relevance and impact**. For this purpose, please describe how it will address the key features of a cross-border SOC platform defined in depth in Section 4.2 of the CfEI.*

Please note that the expression of interest should also take into consideration the eligibility and award criteria displayed in Section 5 of the CfEI.

Please provide, in complement to this Submission Form, official letters of support from the authorities of the participating MS.

2.1 Description of the project, relevance and impact.

Please provide a description of the proposed cross-border SOC platform according to the key features is described in Section0 4.2 of the CfEI.

- **General concept and governance**
- **Interoperability**
- **Data management**
- **Contribution to EU situational awareness**
- **Highly secure infrastructure and state-of-the-art technologies and tools**
- **Provision of other services and activities to strengthen EU detection capabilities**

2.2 Goods and services to be jointly procured and Total cost of acquisition (TCA)

Please provide a description of the proposed cross-border SOC platform according to this key feature, which is described in the award criteria of Section0 6 of the CfEI.

The information should include detailed information about the types of goods and services to be procured through the joint procurement(s) for the purpose of setting up the cross-border platforms and their projected costs.

2.3 Completed model hosting and usage agreement.

Please provide a completed version of Appendix V of the model hosting and usage agreement found in Annex 3 of this CfEI. This will supplement the model hosting and usage agreement with those hosting and usage elements which are specific to this application.

2.4 Coordinator's mandate from each participating Member State

Please provide a completed copy of Annex 4 ('Commitment and Mandate letter') from each participating Member State empowering the consortium's coordinator to act on their behalf. This should contain a commitment to transfer the necessary funds to the coordinator for the purpose of the joint procurement(s) with the ECCC.

2.5 Complementarity with any potential separate application for a grant

Please provide a short description of the complementarity with any potential separate application for a grant to be submitted under the separate call for grant proposals on SOCs[18]

[18] See section DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) in the call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)

By submitting an expression of interest, the participant accepts that, in case of award, certain data like the name, locality and amount (amongst others) will be published.

By submitting an expression of interest, the participants of the consortium accept the terms and conditions set out in the CfEI.

I declare that all information provided in this submission form and its annexes is correct.

Date: Signature of the legal representative of the coordinator organisation

Annex 3. Model hosting and usage agreement

Cross-border Security Operations Centres

Hosting and Usage Agreement

No XX/2022

[name] Coordinator *for hosting and using tools and infrastructures necessary to establish a Cross-border SOC platform*

Table of Contents

The present Hosting and Usage Agreement is concluded between:

on the one part,

The European Cybersecurity Industrial, Technology and Research Competence Centre (hereinafter "ECCC"), represented for the purposes of signature of this Agreement by its interim Executive Director, Miguel Gonzalez-Sancho and by the European Commission, represented by the Director of DG CONNECT Directorate H, Lorena Boix Alonso, and

on the other part,

the "Coordinator", [name]

[Coordinator details]

duly represented for the signature of this Agreement by [name],

representing the following participating partners, on the condition that they have each signed the commitment and mandate letter provided in Annex 4 of the Call for Expression of Interest:

[**Participating partner's name**], established in [legal address],

[same for each participating partner],

hereinafter collectively referred to as the "Parties", and individually as a "Party".

The Coordinator and the other participating partners form the "hosting consortium".

Unless otherwise specified, references to "participating partners" and "hosting consortium" include the Coordinator.

The Parties have agreed to enter into the present Hosting and Usage Agreement.

By signing the Agreement and the commitment and mandate letters where relevant, the **Coordinator and the participating partners agree to implement the Agreement in accordance with all the obligations and terms and conditions** set out below and in the following Appendices:

Appendix I. Minimum requirements of the Hosting Sites

Appendix II. Service Level Agreement

Appendix III. Key Performance Indicators (KPIs)

Appendix IV. Associated Deliverables and Milestones

Appendix V. Hosting and usage elements specific to the Application

which form an integral part of the present Hosting and Usage Agreement (hereinafter referred to as "Agreement").

General Framework

Regulation (EU) 2021/887 of the European Parliament and the Council of 20 May 2021 ("Regulation (EU) 2021/887")[19] establishes the European Cybersecurity Industrial, Technology and Research Competence Centre ("ECCC") and the Network of National Coordination Centres.

In order to reinforce capacities to monitor and detect cyber threats, the Coordinator representing the Participating States in the hosting consortium will procure with the ECCC tools and infrastructures necessary to establish a Cross-border Security Operations Centre Platform ("Cross-border SOC") and shall co-own them. The Union financial contribution shall cover up to 75 % of the acquisition costs of the tools and infrastructures for establishing the Cross-border SOC.

The Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 – 2022 ("Decision")[20] provides that the Union will select entities in Member States that provide the necessary facilities to host and manage cross-border platforms for pooling data on cybersecurity threat between several Member States (data potentially coming from various sources). The ECCC will launch a call for expression of interest which will also build up the planning and design of necessary tools and infrastructures. Building on the call for expression of interest, a joint procurement or a number of joint procurements will be launched to develop and manage capacities for the selected cross-border platforms, including advanced tools and infrastructures to securely share and analyse large data sets and threat intelligence among the selected cross-border platforms (e.g. highly-secure infrastructure or advanced data analytics aimed at significantly improving the ability to analyse large sets of data).

In accordance with the Decision, the ECCC launched a call for expression of interest for the selection of the necessary tools and infrastructures to establish a Cross-border SOC[21]. On the basis of the criteria and process

[19] OJ L 202, 8.6.2021, p. 1–31.
[20] C(2021) 7913 final.
[21] REF:.

specified in the above mentioned call for expression of interest, the Governing Board has selected [identification of the selected Coordinator] referred to above as the Coordinator of the hosting consortium that will host and manage the Cross-border SOC.

The competent authorities of the Participating States to the hosting consortium will cover the share of the total cost of ownership of the tools and infrastructures that is not covered by the Union contribution, either until its ownership is transferred by the ECCC to the Coordinator acting on behalf of all Participating States in the consortium, or until the tools and infrastructures are sold or decommissioned in case there is no transfer of ownership.

The purpose of this Agreement is to lay down the terms and conditions under which the Coordinator, acting as representative of the hosting consortium, will ensure that the tools and infrastructures necessary to establish a Cross-border SOC, and co-owned by the ECCC, will be hosted and used in a manner respecting the interests of the ECCC, including by providing data storage equipment and associated services for the fulfilment and implementation of the ECCC tasks and activities.

I. CHAPTER 1

I.1 Subject matter

1. The subject matter of the Agreement is to define the roles and responsibilities between the Parties regarding the provision of the facilities to host and manage the tools and infrastructures necessary to establish the Cross-border SOC and the provision of the hosting services, which are entrusted by the ECCC, being the co-owner of the tools and infrastructures, to the Coordinator and define the relevant terms and conditions for the long term collaboration between the hosting consortium and the ECCC.

2. The hosting consortium will execute the tasks assigned to it in accordance with the Agreement and its Appendixes.

I.2 Definitions

1. For the purposes of this Agreement the following definitions apply:

a) "Acquisition costs" means the cost of acquiring the tools and infrastructures necessary to establish the Cross-border SOC, and includes shipping as well as the costs of installation and testing of the tools and infrastructures.

b) "Application" means the expression of interest submitted on behalf of a hosting consortium in response to the Call for Expression of Interest.

c) "Call for Expression of Interest" means the procedure followed to select the hosting consortium of the Cross-border SOC.

d) "Confidential information" or "confidential document" means any information or document received by either Party from the other or accessed by either Party in the context of the performance of the Agreement that any of the Parties has identified in writing as confidential. It may not include information that is publicly available.

e) "Conflict of interest" means a situation where the impartial and objective implementation of the Agreement by the Coordinator is compromised for reasons involving family, emotional life, political or national affinity, economic interest, any other direct or indirect personal interest.

f) "Coordinator" means the legal entity which is a National Security Operations Centre, established in a Participating State that is a Member State, which concludes this Agreement as well as any future joint procurement agreement on behalf of all Participating States in the hosting consortium, and which has been selected in accordance with the Call for Expression of Interest.

g) “Decision” means the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 – 2022, and the Annexes thereto.

h) “Force majeure” means any unforeseeable, exceptional situation or event beyond the control of the Parties that prevents either of them from fulfilling any of their obligations under the Agreement which is not attributable to error or negligence on their part or on the part of the subcontractors, affiliated entities or third parties in receipt of financial support and which proves to be inevitable despite their exercising due diligence. Such force majeure events can include, if not proven otherwise, inter alia, terrorist attacks, war or insurrection, natural catastrophes, interruptions in general traffic or data communication. The situation or event must not be attributable to error or negligence on the part of the Parties or on the part of the subcontractors and must prove to be inevitable despite their exercising due diligence. Defaults, defects in equipment or material or delays in making them available, labour disputes, strikes and financial difficulties may not be invoked as force majeure, unless they stem directly from a relevant case of force majeure as set out above.

i) “Formal notification” means a form of communication between the Parties made in writing by mail or email, which provides the sender with concrete evidence that the message was delivered to the specified recipient.

j) “Fraud” means any intentional act or omission by the Coordinator or the hosting consortium affecting the Union’s or the ECCC's financial interests relating to the use or presentation of false, incorrect or incomplete statements or documents, to non-disclosure of information in violation of a specific obligation.

k) “Grave professional misconduct” means a violation of applicable laws or regulations or ethical standards of the profession to which a person or entity belongs, or any wrongful conduct of a person or entity which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence.

l) “Hosting consortium” means a group of Participating States that have agreed to contribute to the acquisition and operation of a Cross-border SOC and any organisations representing these Participating States.

m) “Hosting entity” means a legal entity which will host or manage any part of the tools or infrastructures acquired to establish a Cross-border SOC.

n) “Hosting site” means the physical facilities at which a hosting entity will host or manage the Cross-border SOC and which is established in a Participating State.

o) “Irregularity” means any infringement of a provision of Union law resulting from an act or omission by the Coordinator or an organisation representing the Participating States in the hosting consortium, if any, which has or would have the effect of prejudicing the Union’s or the ECCC’s financial interests.

p) “IT infrastructure” means the set of IT equipment needed for hosting and running the Cross-border SOC.

q) “National SOC” means 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.

r) “Participating partner” means an organisation representing a Participating State in the hosting consortium.

s) “Participating State” means a state which is a member of a hosting consortium.

t) “Related person” means any natural or legal person who is a member of the administrative, management or supervisory body of the Coordinator or its partners, if any, or an economic operator, or who has powers of representation, decision or control with regard to that person.

u) “Subcontract” means a procurement contract within the meaning of Article III.1 of this Agreement, which covers the implementation by a third party of tasks forming part of the Agreement.

v) “Substantial error” means any infringement of a provision of the Agreement resulting from an act or omission, which causes or might cause a loss to the Union’s financial contribution to the ECCC or damage the Union’s or the ECCCs financial interests.

w) “Technical infrastructure” means the set of infrastructure equipment needed for hosting and running the tools, services and IT infrastructures. It includes equipment related to cooling, power supply and distribution, fire security and physical security.

x) “Tools and infrastructures necessary to establish a Cross-border SOC” means any hardware, software or services co-owned by the ECCC with Participating States. This could include, but is not limited to, servers, , micro data center racks, high speed switches, firewall switches, GPUs, HSMs, probes, visualisation tools, SIEM tools, vulnerability managers, aggregation tools, incident reporting tools, situation awareness correlator tools, AI/ML tools, PKI tools, orchestration systems, commercial CTI feeds, AI/ML functionality updates, dedicate service virtual telco line, cloud storage, software development and tuning services, or consultancy services.

y) “Total cost of ownership” of the tools and infrastructures means the acquisition costs plus the other relevant capacity-building costs, including maintenance.

z) “User” or “users” means any natural or legal person, entity or international organisation that has been granted use of the tools and infrastructures.

aa) “Vendor” refers to the person(s) with whom a procurement contract for the acquisition and maintenance of the tools and infrastructures or parts thereof is signed by the procuring parties.

2. Terms not defined herein will have the same meaning as in Regulation (EU) 2021/887.

II. CHAPTER 2

II.1 General Obligations of the Coordinator

1. The Coordinator will:

a) Ensure the participating partners execute their obligations under the Agreement to the highest professional standards respecting deadlines mutually agreed by the Parties.

b) Ensure all activities and services will be carried out by the participating partners in compliance with the applicable health and safety laws and regulations.

c) Ensure the participating partners maintain the functional separation, and to the extent possible, the physical separation of the tools and infrastructures establishing the Cross-border SOC and any national or regional Security Operations Centres they manage.

d) Ensure the participating partners see to it that the personnel performing the obligations under the Agreement possesses the professional qualifications and experience required for the execution of the tasks assigned to them.

e) ensure the proper management of the tools and infrastructures and the IT environment to enable users to access the resources and services for the total duration of the Agreement.

f) ensure the security of the tools and infrastructures, the technical and IT environments and ensure the hosting entities secure their own security.

g) report to the ECCC through the submission of documents and completion of KPIs defined in Appendix III Key performance indicators (KPIs). The KPIs can be modified by the Coordinator and the ECCC by express written agreement of the Parties.

h) apply the usage conditions and rules set up by the ECCC to the Union's usage of the tools and infrastructures on the basis of the relevant decision of its Governing Board.

i) inform the ECCC and users without delay about the incidents impacting the use of the tools and infrastructures or the IT environment.

j) provide any information to the ECCC that is relevant for the ECCC to perform its duties under the present Agreement and Regulation (EU) 2021/887.

k) fulfil its financial obligations as defined in the Agreement.

l) implement the energy efficiency and environmental sustainability measures defined as part of the Technical Specifications of the hosting site(s) on the basis of the Application.

2. The Coordinator will ensure the functionality of the tools and infrastructures, but it will not be liable for incidents or damage attributable to: a) hardware failures or faults of the tools and infrastructures where their origin lies outside the action of the Coordinator, b) software failures or faults where their origin lies outside the action of the Coordinator, c) misuse of the tools and infrastructures by users other than the participating partners d) negligence or failure of users other than participating partners to follow the instructions for use of the tools and infrastructures or breach of the end user license terms, e) instructions or specifications given by the ECCC, or f) force majeure events in accordance with Article IV.6. In all cases, including the above, the Coordinator will inform the ECCC and will take without delay all appropriate measures to restore the functionality of the tools and infrastructures to minimise costs and prevent financial loss or damage to the ECCC and to the tools and infrastructures.

II.2 General Obligations of the ECCC

1. The ECCC will:

   a) Be the co-owner of the tools and infrastructure along with the Participating States of the hosting consortium taking part in a joint procurement, with the share of ownership corresponding to the rate of funding provided in the joint procurement.
   b) Provide any information to the Coordinator that is relevant for the latter to perform its duties under the Agreement within the deadlines agreed by the Parties.
   c) Fulfil its financial obligations as defined in the Agreement and the joint procurement agreement.

II.3 Obligations of the Parties during the acquisition procedure

1. The ECCC, supported by the Coordinator, will launch the process for the acquisition of the tools and infrastructures in accordance with the financial rules of the ECCC.

2. Throughout the acquisition process of the tools and infrastructures, including the preparatory phase, the Parties will work together in a spirit of collaboration for achieving the objective of acquiring the tools and infrastructures.

3. For that purpose, the Parties will have the following responsibilities:

   a. The ECCC and the Coordinator will work together in order to define (design) the main technical specifications of the tools and infrastructures to be acquired.

   b. The ECCC and the Coordinator will agree in the joint procurement agreement upon the detailed practical arrangements for the evaluation of the tenders, the award of the contract, the law applicable to the contract and the competent court for hearing disputes.

   c. The Coordinator will identify and implement the hosting sites' requirements, including but not limited

to the physical infrastructure, security rules and site regulation, for the proper installation and operation of the tools and infrastructures. It is the responsibility of the Coordinator to ensure the hosting entities prepare the hosting sites on time for the installation of the tools and infrastructures. Appendix IV. Associated deliverables and milestones defines the milestones (M2 "Site preparation according to the acquisition procedures of the tools and infrastructures necessary to establish a Cross-border SOC", M3 "Site adaptation to host the tools and infrastructures necessary to establish a Cross-border SOC") required for the installation of the tools and infrastructures. For considering the two abovementioned milestones met in accordance with Appendix IV. Associated deliverables and milestones and within the deadlines set therein, the Coordinator will provide to the ECCC:

i. Evidence of compliance with each requirement and specification as included in Appendix I. Minimum requirements of the Hosting Sites and Appendix V. Hosting and usage elements specific to the Application ;
ii. Evidence of readiness to provide the required services defined in this Agreement;
iii. Evidence of successful testing of all requirements defined in this Agreement;
iv. Demonstration of resilience of systems and components.

4. The ECCC or any mandated entity of the ECCC will have the right to inspect the hosting sites, data centres, documentation, certifications and test reports, where relevant, in order to sign off acceptance of the relevant milestones.

II.4 Obligations of the Parties during the performance of the Agreement

1. Unless otherwise indicated, the Coordinator will be mandated to act in the name and on behalf of the ECCC during the installation, the maintenance and, if necessary, the dismantling of the tools and infrastructures. For the purpose of these technical operations, the Coordinator will be the single point of contact of the vendor in the framework of the procurement contract to be signed with the vendor.

II.4.1 Delivery and installation of the tools and infrastructures

1. The Coordinator will monitor and supervise the proper delivery and installation of the tools and infrastructures by the vendor, in cooperation with the vendor.

2. The Coordinator will provide a report to the ECCC in that regard, and will respond to any questions relevant to the delivery and installation of the tools and infrastructures in a timely manner.

3. The Coordinator will collaborate with the vendor during the installation to make sure that the installation of the tools and infrastructures is done in time and according to the specified requirements of the procurement contract. The vendor will be solely liable for the proper installation of the tools and infrastructures.

4. The Coordinator will supervise, monitor and check the compliance of the equipment/supplies provided by the vendor during the delivery and installation of the tools and infrastructures with the requirements of the procurement contract.

II.4.2 Acceptance of the tools and infrastructures

1. The Coordinator will check the compliance of the tools and infrastructures with the requirements of the procurement contract and perform the acceptance test in that regard.

2. The Coordinator will perform the acceptance test of the tools and infrastructures in accordance with the testing procedure which shall be jointly agreed between the Parties and defined in the contract with the vendor.

3. In case of compliance, the Coordinator will inform the ECCC accordingly, so that the Executive Director of the ECCC can proceed with the authorisation of the payments to the vendor.

4. In case of non-compliance, the Coordinator will inform the ECCC in writing of all defects or errors detected in

the delivery and installation, will identify such defects or errors in sufficient detail and support the ECCC in notifying the vendor about same and/or suggest to the ECCC technical solutions identified following a risk management process. The Coordinator shall have the primary role in interacting with the vendor in order to choose the most appropriate solution to be implemented, in consultation with the ECCC, while keeping it informed throughout the process.

II.4.3 Operations

1. The Coordinator must provide the hosting services defined in Required Hosting Activities in Appendix II Service Level Agreement (SLA).

2. The Coordinator must provide the ECCC regular Service, Utilisation and Performance reports as defined in Appendix IV. Associated deliverables and milestones. The Coordinator must implement the allocation of usage of the tools and infrastructures to the ECCC in accordance with this Agreement.

3. The Coordinator must ensure that the hosting entities meet the KPIs defined in Appendix III Key performance indicators (KPIs).

II.5 End of the operations of the tools and infrastructures

1. At the earliest three years after the successful acceptance test by the Coordinator of the tools and infrastructures installed in the hosting entities, the ECCC, upon mutual agreement of the Parties and subject to decision of the Governing Board, may decide to transfer its share in the ownership of the tools and infrastructures to the Coordinator, or, sell it to another entity or decommission it, in whole or in part.
2. If the ECCC, with the agreement of the Coordinator, decides to transfer the ownership of the tools and infrastructures at the end of its operation, the associated costs will be calculated at that moment in accordance with standard accounting practices for such assets in force at that time. Linear depreciation using a period of 3 years will be applied.

3. In the case of transfer of ownership to the Coordinator in accordance with paragraph 1 before full depreciation of the tools and infrastructures, the Coordinator will reimburse the ECCC the residual value of the tools and infrastructures that are transferred. The residual value will be calculated taking into account the depreciation in accordance with standard accounting practices for such assets in force at that time. In the absence of commonly agreed standards, linear depreciation using a period of 3 years will be applied.

4. If there is no transfer of ownership to the Coordinator but a decision for decommissioning, the relevant costs will be shared equally by the ECCC and the Coordinator.

5. In case of decommissioning of the tools and infrastructures:

    a) The Coordinator will be responsible for the dismantling process, which will be performed by the vendor in accordance with the relevant contract.

    b) The ECCC will have the right to decide how to use the dismantled equipment.

    6. The ECCC will not be liable for any costs incurred after the transfer of ownership of the tools and infrastructures or after its sale to the Coordinator or its decommissioning.

II.6 Conflict of Interest

1. The Coordinator must take all measures to prevent any situation where the impartial and objective implementation of the tasks is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest (“conflict of interest”).

2. The Coordinator must formally notify to the ECCC without delay any situation constituting or likely to lead to a conflict of interest and immediately take all the necessary steps to rectify this situation.

3. The ECCC may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

II.7 Confidentiality obligation and non-disclosure

1. The ECCC and the Coordinator undertake to preserve the confidentiality of any document, information or other material directly related to the subject of the Agreement that is duly classified as confidential.

2. The Parties will not use confidential information and documents for any reason other than fulfilling the obligations under the Agreement, unless otherwise foreseen in writing.

3. A receiving party will notify the disclosing party if it is legally required to disclose any confidential information, or learns of any unauthorized disclosure of confidential information.

4. The Parties will be bound by the obligation referred to in the above paragraphs during the implementation of the Agreement and for as long as the tools and infrastructures remain in the hosting entities under the ownership of the ECCC and for a period of ten (10) years starting from the date of termination of this Agreement, unless:

   a) the concerned Party agrees to release the other Party from the confidentiality obligations earlier;
   b) the confidential information becomes public through other means than in breach of the confidentiality obligation through disclosure by the Party bound by that obligation;
   c) the disclosure of the confidential information is required by law, regulation or binding order of competent authorities.

II.8 Processing of Personal data

II.8.1 Processing of personal data by the ECCC

1. The ECCC will process any personal data under the Agreement in accordance with Regulation (EU) 2018/1725.[22]

2. Where the ECCC is the data controller under Regulation (EU) 2018/1725, such data will be processed by the 'data controller' solely for the purposes of the implementation, management and monitoring of the Agreement or to protect the Union's or the ECCC's financial interests, including checks, audits and investigations, without prejudice to possible transmission to the bodies charged with the monitoring or inspection tasks in application of the applicable rules.

3. The persons whose personal data are processed have the right to access, rectify or erase their own personal data and the right to restrict or, where applicable, the right to data portability or the right to object to data processing in accordance with Regulation (EU) No 2018/1725. For this purpose, they must send any queries about the processing of their personal data to the data controller, via the contact point indicated in the privacy statements that are published on the ECCC and Commission websites.

4. The persons whose personal data are processed may have recourse at any time to the European Data Protection Supervisor.

II.8.2 Processing of personal data by the Coordinator

1. The Coordinator must process personal data under the Agreement in compliance with applicable EU and national law on data protection (including authorisations or notification requirements).

2. The Coordinator may grant its personnel access only to data that is strictly necessary for implementing, managing and monitoring the Agreement. The Coordinator must ensure that the personnel authorised to process personal data has committed itself to confidentiality or is under appropriate statutory obligation of

22 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002, OJ L 295, 21.11.2018, p. 39–98.

confidentiality.

3. The Coordinator must adopt appropriate technical and organisational security measures having regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing of the personal data concerned. This is in order to ensure, as appropriate:
    a) the pseudonymisation and encryption of personal data;
    b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
    e) measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

II.9 Visibility of Union funding and support from Participating States

II.9.1 Information on ECCC funding and support from Participating States – Obligation and right to use the ECCC logo and the EU emblem

1. Unless the ECCC requests or agrees otherwise, any communication or publication made by the participating partners that relates to the tools and infrastructures co-owned by the ECCC, including at conferences, seminars or in any information or promotional materials (such as brochures, leaflets, posters, presentations, in electronic form, etc.), must:
    a. display the ECCC logo,
    b. display the EU emblem, and
    c. include the following text: "The acquisition and operation of the Cross-border SOC is funded jointly by the ECCC, through the European Union's Digital Europe Programme, as well as by the Participating States [countries to be added]".

2. When displayed together with another logo, the ECCC logo and the EU emblem must have appropriate prominence.

3. The obligation to display the ECCC logo and the European Union emblem does not confer to the participating partners a right of exclusive use. The participating partners may not appropriate the ECCC logo and the EU emblem or any similar trademark or logo, either by registration or by any other means.

4. For the purposes of the first, second and third subparagraphs and under the conditions specified therein, the participating partners may use the ECCC logo and the EU emblem without first obtaining permission from the ECCC or the Commission.

II.9.2 Disclaimer

1. Any communication or publication that relates to the Cross-border SOC, made by the participating partners in any form and using any means, must indicate:
    a) that it reflects only the author's view; and
    b) that the ECCC is not responsible for any use that may be made of the information it contains.

II.9.3 Information on support from Participating States

1. Unless the Parties agree otherwise, any communication or publication made by the ECCC that relates to the Cross-border SOCs, shall together with the ECCC logo and the EU emblem, display:
    a) the flag of the Participating States in the hosting consortium,
    b) the logo of the participating partners,

c) include the following text: “The acquisition and operation of the Cross-border SOC is funded jointly by the ECCC, through the European Union’s Digital Europe programme, as well as by the Participating States [countries to be added]”.

2. For the purposes of paragraph 1 and under the conditions specified therein, the ECCC may use the logo of the participating partners without first obtaining their permission.

II.10 Security

1. The Coordinator shall ensure that the hosting entities provide access to the tools and infrastructure for the purposes stipulated in this Agreement, while ensuring the security of the tools and infrastructures and prevent unauthorised use by all means. These should include as a minimum the physical and IT security measures described in Appendix I. Minimum requirements of the Hosting Sites.

2. The Coordinator must ensure that the hosting entities adopt appropriate technical and organisational security measures having regard to the risks inherent to the hosting and operations of such tools and infrastructures. This will include the functional separation, and to the extent possible, the physical separation of the tools and infrastructures and any national or regional Security Operations Centre the hosting entities manage.

3. The security requirements will be those defined in Appendix V. Hosting and usage elements specific to this application.

II.11 Financial obligation

II.11.1 Acquisition costs of the tools and infrastructures

1. The Union’s financial contribution to the acquisition of the tools and infrastructures is set at a maximum of EUR XXX. The Union’s financial contribution will cover up to 75 % of the acquisition costs up to the maximum budget.

2. The remaining acquisition costs of the tools and infrastructure will be covered by Participating States in the hosting consortium.

3. The contribution by Participating States in the hosting consortium must be transferred to the Coordinator, who will transfer the funds to the ECCC.

4. The Coordinator must transfer the total contribution of the hosting consortium to the ECCC at least 2 months ahead of the respective payments to the vendor.

5. Within the budget agreed, the ECCC will send at any time it deems necessary a payment request to the Coordinator (the “Payment Request”) to cover the commitments for the acquisition of the tools and infrastructures taking into account the schedule of payments agreed between the procuring parties and the vendor.

II.12 Checks and Audits

II.12.1 General obligations

1. The ECCC may, during the implementation of the Agreement or afterwards, carry out technical and financial checks and audits to determine that the Coordinator and the other participating partners are implementing the Agreement properly and are complying with the obligations under the Agreement, including assessing deliverables and reports. For that purpose, the Coordinator must provide any information, including information in electronic format, requested by the ECCC or by any other outside body authorised by the ECCC. Information provided must be accurate, precise and complete and in the format requested, including electronic format.

2. The checks and audit data must be protected, non-repudiated and restricted to authorized staff. Relevant records will be retained online for at least ninety (90) days and further preserved offline for a period of the

agreement or as required by the ECCC.

3. Information and documents provided as part of checks or audits must be treated on a confidential basis.

4. The above checks and audits may be carried out either directly by the ECCC's own staff or by any other outside body authorised to do so on its behalf.

5. In addition to the ECCC, the European Commission, the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO) and the Court of Auditors may carry out checks and audits in accordance with their respective competences and the applicable legal framework.

6. For actions funded from the Digital Europe Programme, audits of recipients of Union funds should be carried out in compliance with Regulation (EU) 2021/694.

II.12.2 On-the-spot visits

1. The ECCC has the right to perform on-the-spot visits to the hosting sites and the premises of the hosting entities.

2. During an on-the-spot visit, the hosting entity will allow the staff of the ECCC and any external personnel authorised by the ECCC to have access to the hosting site and premises of the hosting entity, and to all the necessary information related to the hosting and operation of the tools and infrastructures for the assessment of the fulfilment of this Agreement, including information in electronic format.

3. The hosting entity must ensure that the information is readily available at the moment of the on-the-spot visit and that information requested is handed over in an appropriate form. Visits agreed herein will be notified at least seven (7) calendar days beforehand and be carried out in a way that causes minimal disruption to safety and operation of services under the hosting entity's responsibilities.

III. CHAPTER 3

III.1 Subcontracting and third parties

1. The Coordinator is allowed to subcontract certain activities to be performed to third parties. However, the Coordinator must ensure that the percentage of subcontracting activities is proportionate and justifiable in accordance with the objective of the Agreement. The Coordinator will remain bound by its obligations under the Agreement and will be solely responsible for the proper performance of this Agreement, including by third parties acting in their capacity as subcontractors.

2. The Coordinator will make sure that the subcontract does not affect rights and guarantees granted to the ECCC by virtue of this Agreement.

IV. CHAPTER 4

IV.1 Consequences of non-compliance with obligations

1. The Coordinator will use its best endeavours to fulfil its obligations under this Agreement and provide the hosting site services under the highest professional standards and in a timely manner, within the deadlines agreed between the Parties.

2. The ECCC will use its best endeavours to fulfil its obligations under this Agreement in a timely manner, within the deadlines agreed between the Parties.

3. The ECCC and the Coordinator will use their best efforts to solve any non-compliance issue amicably, taking into account the best interests of the Union, the interests of the Coordinator and the hosting consortium and the shared objectives of the ECCC and the Coordinator.

4. In case one of the Parties is not in position to fulfil its obligations under this Agreement on time for whichever reason, it will notify the other Party without delay, stating the nature of the circumstances, their likely duration and effects and the measures taken to limit or mitigate any damage.

5. In case a status report shows that the services provided by the Coordinator are not fully compliant with this Agreement, the ECCC will evaluate the severity of the problem and its consequences, and discuss the conclusions of this evaluation with the Coordinator.

6. If the obligations of the Coordinator included in this Agreement have not been implemented accordingly or if any obligation under the Agreement has been breached by the Coordinator, the ECCC will send a formal notification to the Coordinator requesting the Coordinator to rectify that situation or provide explanations and intended rectification or remedial actions. The Coordinator will respond to this notification within ten (10) calendar days following the date of receipt.

7. If the Coordinator does not respond within the abovementioned timeframe, the ECCC will send a reminder by way of a second formal notification to the Coordinator, specifying the measures it intends to take if the Coordinator does not respond to its request or does not take appropriate and reasonable measures to rectify the situation. The Coordinator must respond to this second formal notification within ten (10) calendar days following the date of receipt. If the Coordinator does not respond to this reminder, the ECCC will have the right to take the measures described in paragraph 8 and in Article IV.2, notwithstanding any other legal rights of the ECCC.

8. In all cases, including cases of force majeure, the ECCC will have the right to request from the Coordinator to comply with the Agreement, take remedial measures and/or proportionally reduce or recover amounts unduly paid to the Coordinator, as appropriate and in accordance with the principle of proportionality and the seriousness of the breach or non-compliance and after using its best endeavours to allow the Coordinator to exercise its right to be heard.

9. Before the ECCC proceeds as described in paragraph 8 of this Article, it will send a formal notification to the Coordinator which will include the following information:
    a. the measures it intends to take and the start date of their application;
    b. the ECCC's intention to reduce any amount to be paid and the corresponding amount;
    c. the reasons for reduction and/or other measures; and
    d. invitation to the Coordinator to submit observations within ten (10) calendar days following the date of receipt of the formal notification.

10. In all cases, where the fault, situation or event is attributable to error or negligence on the part of the vendor and in cases referred to in II.1 paragraph 2, the Coordinator shall not be considered as non-compliant, in breach of its obligations or liable.

IV.2 **Liquidated Damages**

1. If the Coordinator fails to perform its obligations within the applicable time limits as set out in this Agreement, and such cases constitute significant and/or recurring and/or persistent non-compliance or breach of the obligations under the Agreement, the ECCC, taking the principle of proportionality into account, may claim liquidated damages for each day or hour of delay using the following formula:

$$0{,}20 * (RH * h)$$

Where RH is the cost of a Running Hour, to be understood as the cost of running the cross-border platform for one hour.

And h is the duration in hours of the non-compliance or breach of the obligations under the Agreement. The maximum amount of liquidated damages payable per each calendar year will be limited to one

million euro (1.000.000 €).

2. The amount of such liquidated damages that results from the application of the formula above may be reduced by the ECCC if it is considered justified by the seriousness of the breach and the specific character and circumstances of the non-compliance or breach, taking the principle of proportionality into account.

3. Liquidated damages may be imposed in addition to other reductions in the Union's financial contribution.

4. The ECCC must formally notify the Coordinator of its intention to apply liquidated damages and the corresponding calculated amount.

5. The Coordinator will have thirty (30) calendar days following the date of receipt to submit observations. Failing that, the decision of the ECCC becomes enforceable the day after the deadline for submitting observations has elapsed.

6. If the Coordinator submits observations, the ECCC, taking into account the relevant observations, must notify the Coordinator:
    a. of the withdrawal of its intention to apply liquidated damages; or
    b. of its decision to reduce the amount of the liquidated damages as appropriate; or
    c. of its final decision to apply liquidated damages and the corresponding amount.

7. The Parties expressly acknowledge and agree that any amount payable under this Article is not a penalty and represents a reasonable estimate of fair compensation for the damage incurred due to failure to provide the services within the agreed time limits set out in this Agreement.

8. Any claim for liquidated damages does not affect the Coordinator's actual or potential liability or the ECCC's rights under other articles in this Agreement.

IV.3 **Liability**

1. The ECCC will not be liable for any damage or loss caused by the Coordinator or any participating partner, including any damage or loss to third parties during or as a consequence of performance of the Agreement, and the operation of the tools and infrastructures on its behalf, unless the loss or damage was caused by wilful misconduct or gross negligence by the ECCC.

2. The Coordinator will assume full liability towards the ECCC for the performance of its obligations under this Agreement as a whole, including financial and operational liability. In case of a hosting consortium, only the Coordinator will be fully liable towards the ECCC for the performance of the Agreement.

3. When determining the liability of the Coordinator under the Agreement the principle of proportionality shall be applied and the seriousness of the breach or non-compliance shall be taken into account.

4. The Coordinator will be liable for any loss or damage caused to the ECCC during or as a consequence of the performance of the Agreement. The aggregate maximum liability for damages of the Coordinator based on the Agreement will not exceed the residual value of the tools and infrastructures, including possible liquidated damages. However, if the damage or loss is caused by the gross negligence or wilful misconduct of the Coordinator or one or several other participating partners, or of any of the participating partners' personnel or subcontractors, as well as in the case of an action brought against the ECCC by a third party, the Coordinator will be liable for the whole amount of the damage or loss.

5. If a third party brings any action against the ECCC in connection with the performance of the Agreement, the Coordinator must closely collaborate and assist the ECCC in the legal proceedings, including by intervening in support of the ECCC upon request.

6. If the liability of the ECCC towards the third party is established and such liability is caused by the Coordinator

during or as a consequence of the performance of the Agreement, paragraph 2 applies.

IV.4 **Insurance**

1. The Coordinator must take out an insurance policy to cover the operation of the hosting sites and of the tools and infrastructure and against risks and damage or loss relating to the performance of the tools and infrastructures. It must also take out supplementary insurance as reasonably required by standard practice in the industry. Upon request, the Coordinator must provide evidence of insurance coverage to the ECCC.

IV.5 **Termination of the Agreement**

1. The Agreement may be terminated by mutual consent of the Parties in case the subject matter of this Agreement has been fulfilled or becomes impossible to fulfil.

IV.5.1 Termination by the ECCC of the Agreement for specific reasons

1. The ECCC may terminate the Agreement if the Coordinator does not remedy within sixty (60) calendar days from written notification any material or serious breach or non-compliance issue falling under its responsibility concerning the following situations, unless manifestly such breach or non-compliance cannot by its nature be remedied:
   a) the Coordinator or any person that assumes unlimited liability for the debts of the Coordinator is in one of the situations provided for in points (a) and (b) of Article 136(1) of the EU Financial Regulation[23];
   b) the Coordinator is subject to any of the situations provided for in points (c) to (f) of Article 136(1) or to Article 136(2) of the EU Financial Regulation;
   c) the procedure for selecting the Coordinator proves to have been subject to substantial errors, irregularities or fraud;
   d) the Coordinator does not comply with applicable obligations under environmental, social and labour law established by Union and Community law, national law, collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU[24];
   e) the Coordinator is in a situation that constitutes a conflict of interest or a professional conflicting interest as referred to in Article II.6;
   f) a change to the Coordinator's legal, financial, technical, organisational or ownership situation is likely to substantially affect the implementation of the Agreement in an adverse manner;
   g) the Coordinator does not comply with or is in serious breach of its obligations under this Agreement.

IV.5.2 Procedure and effect of termination

1. One Party must formally notify the other Party of its intention to terminate the Agreement and the grounds for termination. The termination will become effective on the date on which the tools and infrastructures will no longer be hosted in the premises of the relevant hosting entity, unless otherwise agreed by the Parties, taking into account the grounds for termination.

2. In such case, at the request of the ECCC and regardless of the grounds for termination, the Coordinator must provide all necessary assistance, including information, documents and files, to allow the ECCC to transfer the tools and infrastructure to a new location, with minimum interruption or adverse effect on the quality or continuity of the operation of the tools and infrastructures. The Parties may agree to draw up a transition plan detailing the transfer of the tools and infrastructures.

3. In cases where the Agreement has been terminated on the grounds that the Coordinator does not comply

[23] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012, OJ L 193, 30.7.2018, p. 1–222

[24] OJ L 94 of 28.03.2014, p. 65.

with its obligations under this Agreement, the Coordinator must provide such assistance at no additional cost, except if it can demonstrate that it requires substantial additional resources or means or otherwise causes additional expenses, in which case it must provide an estimate of the costs involved and the Parties will negotiate an arrangement in good faith.

4. If the Agreement has been terminated on the basis of Article IV.5.1, the Coordinator will be liable for direct damages incurred by the ECCC as a result of the termination of the Agreement, including the cost of transferring the tools and infrastructures to another hosting entity, unless the damage was caused by force majeure.

5. In any case, the Parties must take all appropriate measures to minimise costs and prevent damage to the other Party and to the tools and infrastructures.

IV.6 **Force majeure**

1. If a Party is affected by force majeure, it must immediately notify the other Party, stating the nature of the circumstances, their likely duration and the foreseeable effects.

2. The Party faced with force majeure may not be considered in breach of its obligations under the Agreement if it has been prevented from fulfilling them by force majeure. The Parties must take all reasonable measures to limit any damage due to force majeure. They must do their best to resume the implementation of the action as soon as possible.

V. **CHAPTER 5**

V.1 **Entry into force and duration**

1. The Agreement shall enter into force on the date on which it is signed by the last Party and will remain in force until either the ownership of the tools and infrastructures is transferred by the ECCC to the Coordinator or until the tools and infrastructures are sold or decommissioned in case there is no transfer of ownership, and at the latest until 31.12.2029.

2. The extension of the duration of the present Agreement is subject to the express written agreement of both Parties.

V.2 **Amendments**

1. Any amendment to the Agreement must be made by mutual agreement of the Parties in writing.

2. Any amendment must not make changes to the Agreement that might alter its purpose.

3. Any request for amendment must be duly justified and must be sent to the other Party in due time before it is due to take effect, except in cases duly substantiated by the Party requesting the amendment and accepted by the other Party.

4. Amendments will enter into force on a date agreed by the Parties or, in the absence of such an agreed date, on the date on which the last Party signs the amendment.

V.3 **Severability**

1. Each provision of this Agreement is severable and distinct from the others. If a provision is or becomes illegal, invalid or unenforceable to any extent, it must be severed from the remainder of the Agreement. This does not affect the legality, validity or enforceability of any other provisions of the Agreement, which continue in full force and effect. The illegal, invalid or unenforceable provision must be replaced by a legal, valid and enforceable substitute provision which corresponds as closely as possible to the real intent of the Parties. The replacement of such a provision must be made in accordance with Article II.7. The Agreement must be

interpreted as if it had contained the substitute provision as from its entry into force.

V.4 **Applicable law and settlement of disputes**

1. The Agreement is governed by Union law, supplemented for any matter not covered by the Regulation or by other Union legal acts by the law of Romania.

2. The Parties will endeavour to settle amicably any dispute or complaint relating to the interpretation, application or validity of the Agreement. Any dispute which cannot be settled amicably must be submitted to the jurisdiction of the General Court or, on appeal, the Court of Justice of the European Union.

3. Nothing in the Agreement will be interpreted as a waiver of any privileges or immunities which are accorded to the ECCC by its constituent act.

V.5 **Communication between the Parties**

V.5.1 Communication Details

1. For the purpose of this Agreement, communications must be sent to the following addresses:

    1. ECCC:

        [address of ECCC]

    2. Coordinator:

        [Address of Coordinator]

V.5.2 Form and means of communication

1. Any communication of information, notices or documents under the Agreement must:
    a. be made in writing in paper or electronic format in the language of the Agreement;
    b. bear the Agreement number;
    c. be made using the relevant communication details set out above; and
    d. be sent by mail or email.

V.5.3 Date of communications by mail and electronic mail (email)

1. Any communication is deemed to have been made when the receiving Party receives it, unless this Agreement refers to the date when the communication was sent.

2. Email is deemed to have been received on the day of dispatch of that email, provided that it is sent to the email address indicated in Article V.5.1. The sending Party must be able to prove the date of dispatch. In the event that the sending Party receives a non-delivery report, it must make every effort to ensure that the other Party actually receives the communication by email or mail. In such a case, the sending Party is not held in breach of its obligation to send such communication within a specified deadline.

3. Mail sent to the ECCC is deemed to have been received by the latter on the date on which the ECCC registers it.

4. Formal notifications are considered to have been received on the date of receipt indicated in the proof received by the sending Party that the message was delivered to the specified recipient.

VI. **SIGNATURES**

IN WITNESS WHEREOF the undersigned, being duly authorized, have signed this Hosting and Usage Agreement.

SIGNATURES

For the Hosting Entity
[name],
[function]

Done in English
In , on the date of

For the ECCC
Miguel Gonzalez-Sancho,
Interim Executive Director

Done in English, in , on the date of

For initial actions until the ECCC has the capacity to implement its own budget:
This Hosting and Usage Agreement is also signed by the European Union, represented by the Commission. However, the European Union will cease to be a contracting party from the moment the ECCC has the capacity to implement its own budget.

For the Commission
Lorena Boix Alonso,
Director of DG CONNECT

Done in English, in , on the date of

Appendix I. Minimum requirements of the Hosting Sites

The following list provides the minimum requirements for the hosting entities to host the necessary tools and infrastructures to establish a cross-border SOC platform. The hosting site must be able to guarantee the following within the timeline for the installation of the tools and infrastructures:

1. Power capacity and power quality appropriate for the operation of the proposed platform.
2. UPS power available to cover the critical systems including storage and access to data of the cross-border platform.
3. At least 100 m² of contiguous raised floor space available for the hosting the operational platform (dana centre if required + offices)
4. Minimal requirements for physical access security:
    i. Operated reception and ability to limit or restrict physical access to the Cross-border platform
    ii. badge access with differentiated access areas (Layered security zones)
    iii. video surveillance
    iv. intrusion detection
5. Minimal requirements regarding fire mitigation:
    v. fire detection
    vi. fire extinguishing mechanism
    vii. operational procedures to deal with fire and minimize damage to equipment and persons
6. Minimum requirements regarding IT access security:
    viii. intrusion detection
    ix. firewalling
    x. network segmentation
    xi. activity / traffic monitoring and traceability
    xii. user authentication and user authorisation
    xiii. vulnerability scanning and monitoring
    xiv. security awareness and training
7. Existence of a dedicated on-call service team for IT issues
8. Existence of a dedicated on-call service team for facilities issues
9. At least 10 Gbit/s redundant connectivity towards the rest of the Internet (link capacity)
10. A mechanism to regularly measure the quality of the services delivered

Appendix II Service Level Agreement (SLA) - Required Hosting Activities

The Coordinator is required to provide the following services relevant to the hosting of the cross-border SOC platform:

a) Provide the Technical Environment including all facility management needed to the operation of the Cross-border SOC platform.

b) Supervise, monitor and check the performance of the commitments and obligations of the vendors that relate to the delivery, installation and maintenance of the platform.

c) Allow consortia members (and other consortia when pertinent) to access and use the services, information and tools put at disposal through the Cross-border SOC platform.

d) The Coordinator undertakes to provide at least the following services:

   a. Hotline/helpdesk and support services, to provide users with a contact point in order to get help for the use of the system and IT environment. This support should be organized as follows:

      i) A single point of a two-level support at least in English which can be contacted by phone and email should be set-up.

      ii) This hotline/helpdesk should answer to requests about difficulties/issues dealing with the use of the Cross-border SOC platform and any information about this Cross-border SOC platform.

      iii) A SOC team composed by highly qualified cyber-security experts and cyber-threats analysts implementing the core of the detection capabilities of the platform.

      iv) An early warning service able to notify in near-to-real-time to the members of the consortia the detected warning and threats.

   b. Access to the Cross-border SOC platform resources by the users;

   c. User documentation (preferable in the form of an online knowledge base), including manuals and other information and tools that are required by the users;

   d. Incident management;

   e. User account management ;

   f. Data storage services (scratch and related temporary storage services);

   g. Data post-processing, including software tools to post-process data;

   h. User support for code porting and optimization (under the terms agreed separately with the ECCC) especially for what concerns AI analysis tools;

   i. Data processing and visualization services (under the terms agreed separately with the ECCC);

   j. Information to users and the ECCC about incidents impacting the use of the Cross-border SOC platform or the IT environment;

   k. At least yearly measurement of user satisfaction with the service offered by the Coordinator via user surveys;

l. At least yearly measurement of the quality of the feeds received/shared by the members of the platform

e) The Coordinator undertakes to provide support related to the Cross-border SOC platform. This must include:

a) On call service support teams for IT issues available to users;

b) Dedicated on-call service team for facilities issues available to users;

c) The Coordinator must have in place an escalation process (both functional and hierarchical) designed to bring appropriate authority and expertise rapidly into play to resolve issues and problems in accordance with agreed service levels, and to quickly answer to cross-border cyber-warnings;

d) Once an incident has been raised, the Coordinator support team will do the utmost to resolve, repair and restore services to full operation within the defined Service Level Agreement time limits.

f) The Coordinator undertakes to report to the ECCC through the production of documents and KPIs reports defined in Appendix IV (Associated deliverables and milestones).

g) The Coordinator undertakes to monitor the IT infrastructure and technical infrastructure and equipment, including power electrical systems

h) The Coordinator undertakes to monitor the capacity and operational load of the hosting site infrastructure providing services to the Cross-border SOC platform.

i) Cooling and other infrastructure services related to the operation of the Cross-border SOC platform, such as fire detection, monitoring, security, at the hosting sites of the Cross-border SOC platform.

j) Provision of electricity consumption of the Cross-border SOC platform and other IT equipment and by the facility (cooling, heating losses ...) related to the operation of the Cross-border SOC platform, taking into account the Power Usage Effectiveness (PUE).

k) Provision of the hosting site infrastructure, including equipment required for running the Cross-border SOC platform. This involves network at the data centre level, different storage subsystems (e.g. high-performance and short-term storage tiers, backup systems and other IT equipment like licence servers etc.).

l) Provision of External Network Connectivity: Connectivity for the Cross-border SOC platform to any external site, including the rest of the Union will require access to an adequate physical networking infrastructure in conformity with the requirements of this hosting and usage agreement.

m) Provision of power back up and distribution items related to providing power to the Cross-border SOC platform installed inside the data centre technical area according to the requirements of this hosting and usage agreement.

n) Provision of long term data storage to fulfil the requirements of the Cross-border SOC platform during the duration of this hosting and usage agreement.

o) Ensure the security of the hosting entities, the Technical and IT Environments and the Cross-border SOC platform. As a minimum, the IT security must include the security measures defined in Appendix 2 “Minimum requirements of the Hosting Sites”

p) Apply the access-time as instructed by the ECCC to the Cross-border SOC platform and to its IT environment

q) Put in place a certified audit procedure covering the operational expenses of the Cross-border SOC

platform and the access-times of the users and to submit an audit report and data on access time once a year to the ECCC's Governing Board.

Appendix III Key performance indicators (KPIs)

The following KPIs apply for the services provided by the Coordinator to the ECCC and defined in this Agreement:

No	KPI	Description	Target value	Period for computing of figure	Resp. when operation
1.	Availability of the Cross-border SOC platform	Fraction of time the system is fully usable (able to operate in normal performance) and available to users Includes: files systems, home directories, login nodes, access network.	> 95 % (monthly basis) for the first 3 months of operation >97% (monthly basis) for the remaining of the operational period	Monthly	Coordinator
2.	Scheduled maintenance of the Cross-border SOC platform	Maintenance is considered as scheduled if users are warned at least 1 week in advance	not more than 5 days per year	Monthly	Coordinator
3.	Stability of performances of the Cross-border SOC platform	Regular execution of a set of benchmarks	> 90 % of the performances measured after the installation of the supercomputer	Every two years	Coordinator
4.	Availability of the critical auxiliary IT equipment	IT equipment necessary for the usage of the Cross-border SOC platform (example: network access, homes…)	> 95 % (monthly basis) for the first 3 months of operation >97% (monthly basis) for the remaining of the operational period	Monthly	Coordinator
5.	Usage of the Cross-border SOC platform	Measured in term of montlhy access to the platform by the consortia members	>>75% of the number of consortia members	monthly	ECCC + Coordinator
6.	Volume of weekly data sharing	Amount of data collected by the platform	Absolute value, and average per number of consortia members	weekly	Coordinator
7.	Quality of data	Accuracy of the provided data	Number of malformed/incomplete information shared/total amount of data shared	Yearly	Coordinator

8.	Platform effectiveness	Number of events detected thanks to the use of the platform	Number of events detected thanks to the use of the platform	monthly	Coordinator
7.	Handling of tickets	A ticket is considered as solved only once the user agrees or has failed to respond to two requests to close the ticket. Providing workaround is acceptable if the workaround has no major negative consequence	70% should be solved in less than 2 working days, 20% in less than 5 working days, the remaining 10% in less than 1 month	Monthly	Coordinator

		Help desk on duty all business days from 8:00 to 18:00 (CET)	(if the number of ticket is less than 10 per month)		
8.	Availability of the facility	Cooling, power supply, fire security.	> 99 % on a monthly basis No more than 5 days of maintenance per year	Monthly	Coordinator
9.	Availability of external connectivity	External connectivity	> 99 % on a monthly basis No more than 5 days of maintenance per year	Monthly	Coordinator
10.	Average number of critical Incidents affecting users (per type of active user)	This KPI will be measured during the first year of operation without committed SLA. After one year, based on the experience gathered, the target SLA could be reviewed.	Average must be lower than 0.5 per month. Based on the number of active users per month. 1 incident affecting several users is only accounted for 1	Monthly	Coordinator
11.	User Satisfaction	Measure of user satisfaction via user survey. The Survey will be jointly defined by the ECCC and the Hosting Entity.	Overall user satisfaction must be over 7 in an scale 0-10	Yearly	Coordinator

Table 1. KPIs

When reported, along with the KPI values, the KPIs must indicate as a minimum:

1. number of problems reported and scheduled or planned downtime experienced;
2. any incidents or changes to the resources such as power failures, security incidents and network performance; and
3. any other impact on normal operations of the resources

If a KPI is not met, the Coordinator has to provide an explanation of the reason/justification together with the corrective action as part of the KPI report to the ECCC.

1. Service Hours

The Cross-border SOC platform services provided to users must be available 24 hours, 7 days per week, except when there is maintenance.

The Coordinator must provide support to users in accordance with point 5 below.

2. Service Availability

1. For the provision of the Service covered by the Coordinator, availability is determined by the percentage of fully usable time (able to operate in normal performance) and available to users. It must include at least the compute nodes, login nodes, network access, file systems and access to home directories.
2. The Coordinator will seek 100 % availability, and meeting the availability defined in the KPIs.
3. The Coordinator will calculate “Service Unavailability” in a calendar month. “Service Unavailability” consists of the number of minutes that the service was not available to Users, and includes unavailability associated

with any maintenance at the hosting site other than Scheduled Maintenance. Outages will be counted as Service Unavailability even if users do not open an incident with support during or after the outage. Service unavailability will not include Scheduled Maintenance, or any unavailability resulting from:

a) acts or omissions of the ECCC or any use or user of the service authorised by the ECCC;

b) deliberate acts or gross negligence of a User or an End User or reasons of Force Majeure.

4. In the case of a malfunction involving a total unavailability exceeding 24 hours of the Cross-border SOC platform or its IT environment, the Coordinator must inform the ECCC no later than 48 hours after the commence of the incident and a crisis unit would be set up between Coordinator and the ECCC.

- **Availability of external connectivity**

1. The Coordinator must ensure the Cross-border SOC platform's external connectivity. The Coordinator will seek 100 % availability for external connectivity and meet the availability defined in the KPIs.

2. The Coordinator must ensure that there are not more than 5 days of maintenance per year.

3. Performance Testing

1. The Coordinator must take all necessary measures to ensure the performance of the Cross-border SOC platform. In order to test and review it a set of benchmarks must be executed regularly (at least every 2 years) in the Cross-border SOC platform, trying to minimise its service availability. Every time the set of benchmarks is executed, the benchmarks must achieve at least a 90 % of the performances measured after the installation of the Cross-border SOC platform. These will be reviewed as part of the yearly reports. Potential issues not attributable to the Hosting Entity shall be resolved by the vendor of the Cross-border SOC platform or other relevant support providers. must be executed regularly (at least every 2 years) in the Cross-border SOC platform, trying to minimise its service availability. Every time the set of benchmarks is executed, the benchmarks must achieve at least a 90 % of the performances measured after the installation of the Cross-border SOC platform. These will be reviewed as part of the yearly reports. Potential issues not attributable to the Coordinator shall be resolved by the vendors of the Cross-border SOC platform components or other relevant support providers.

4. Regression testing

1. The Coordinator must provide when possible regression testing. The regression testing should be applied when significant changes have been applied to the Cross-border SOC platform to verify that previous applications still work with the new changes.

5. Support Hours

1. Support must be available from 8:00 AM to 6:00 PM (CET), Monday through Friday, except when the facilities are closed due to holidays, administrative closings, or inclement weather. A service can be requested or an Incident reported by telephone during working hours, or by mail or by a Web Portal at any time. Incidents reported or services requested outside the working hours will be served at the next scheduled working day, unless a special procedure for Major Incident is invoked.

6. Incident Escalation

1. In case of operational issues affecting the availability of the services provided to users:

a) The Coordinator will inform without delay the ECCC and propose corrective actions.

b) The Coordinator will assess the severity of the issue and its impact on the users of the ECCC.

c) The ECCC and the Coordinator will agree on the actions to be implemented.

d) The Coordinator will monitor their implementation and provide feedback to the ECCC.

7. Usage of the Cross-border SOC platform

1. The Coordinator must measure the usage of the Cross-border SOC platform and provide the information in a monthly basis. The purpose is to ensure the maximum possible utilisation of the platform. The usage does not include unavailability and scheduled maintenance periods and performance tests when executed. This is measured as part of the monthly KPIs.

8. Backups

1. The Coordinator must ensure that they have a properly backup policy that has been approved by the ECCC with onsite and offsite backup solutions that ensures that the functioning of the Cross-border SOC platform can be restored to a state that can provide back service to customers in case of user or system error. The Coordinator must ensure a backup retention policy of at least 1 month to the users. However, the users shall be responsible for taking their own backups and HE shall not be liable for any adverse effects of any data loss, unless otherwise specified in the relevant user terms and data processing agreement.

9. Monitoring

1. To verify the Cross-border SOC platform and services availability, the Coordinator must have proper monitoring systems (active or passive or combination of both) that provide regularly feedback about the status of the Cross-border SOC platform and related equipment and services. The monitoring system must be used to provide statistics about the service availability and downtimes.

10. Maintenance

2. Scheduled Maintenance means any maintenance at the Cross-border SOC platform that affects the users and that is notified at least one (1) week in advance. Notice of Scheduled Maintenance will be provided to users and the ECCC's designated point of contact via email and other communication systems (e.g. portal).

3. The maintenance program including their maintenance windows should be available to all users and the ECCC.

4. The Coordinator will use reasonable efforts to coordinate with possible impacted users when planning any maintenance to minimise impact to users.

5. "Emergency Maintenance" means any maintenance by the Coordinator, its subcontractors or service providers that does not meet the definition of Scheduled Maintenance. No notice will be required or provided for Emergency Maintenance.

11. Reporting

1. The Coordinator must provide regular reports as deliverables. The list of deliverables is indicated in Appendix IV. Associated deliverables and milestones. The Status Reports must be submitted to the ECCC no later than the 15th of the subsequent month. The due dates for delivery of the Reports are indicated in the same Appendix IV. Associated deliverables and milestones .

2. Status reports will allow assessing if the services provided by the Coordinator are compliant with the specifications listed in Appendix IV. Associated deliverables and milestones and with the KPIs listed in Appendix III Key performance indicators (KPIs). Each quarterly status report will contain, broken down per month, at least the information requested in Appendix IV. Associated deliverables and milestones.

3. This report must include KPIs and status of shared resources used by the Cross-border SOC platform and its users. In case a KPI is not met, the reason should be documented, together with the actions

implemented to solve it.

4. The annual report must summarise at least the information above for one entire year.

Appendix IV. Associated deliverables and milestones

The services provided by the Hosting Entity to the ECCC and the achievement of milestones (see the table below) will be reviewed based on monthly status reports provided by the Hosting Entity to the ECCC.

Service Reporting must include at least:

a) Performance against service targets (Including SLAs)

b) Relevant information about significant events including at least major incidents, deployment of new or changed services.

c) Access time allocation

d) Detected non-conformities against the requirements of this Agreement

e) Customer satisfaction measurements, service complaints and results of the analysis of satisfaction me asurements and complaints.

f) Workload characteristics including volumes and periodic changes in workload.

g) Trend Information on the performance, data sharing volume, events detection

The Coordinator must provide the following periodic deliverables:

Ref.	Periodicity	Title of deliverable	Due date
KPI_month	Monthly	Monthly KPI report for previous month	15th of the next month
PR_month	Monthly	Monthly Performance and utilisation report for the previous month (Table 2. Performance and utilisation Reporting values of the Supercomputer)	15th of the next month
AR_year	Yearly	Audit report and data on the use of access time in the previous financial year	31st March
CR_year	Yearly	Audit report and data on the operation costs in the previous financial year. (Using agreed calculation method)	31st March

Table 3. Periodic deliverables

In addition to the deliverables stated above, the Coordinator has to meet the following milestones:

Ref.	Milestone	Due date
M1	Nomination by the Hosting Entity of the team for collaboration with the ECCC on the acquisition process	(To be filled)
M2	Site preparation accordingly to the acquisition procedures of the Cross-border SOC platform	31 March 2023
M3	Site adaptation to host the Cross-border SOC platform	31 May 2023

Table 4. Milestones

In case a milestone is not reached on time, the ECCC will have the right to reject further deliverables.

Appendix V. Hosting and usage elements specific to the Application

To be completed by applicants to the Call for Expressions of Interest

The contents of Appendix V of the hosting and usage agreement are subject to modifications based on further discussions between the ECCC and the relevant applicants.

When submitting an application to the Call for Expressions of Interest, please define the hosting and usage obligations of the ECCC and the Coordinator in each of the following areas, as relevant to your application.

a) Contribution to EU situational awareness (sharing of data with relevant EU entities):

b) Sharing of correlation analysis tools:

c) Sharing of training/testing platforms:

d) Contribution to cybersecurity data lakes:

Annex 4. Commitment and mandate letter (to be completed by each partner participating in the consortium)

I, the undersigned,

[forename and surname of the legal representative of the future partner signing this mandate],

representing,

[full official name of the future partner] *[ACRONYM]*

[*official legal status or form*][25]

[*official registration No*][26]

[full official address]

[*VAT number*],

('the partner'),

for the purposes of signing and implementing the Hosting and Usage Agreement and any other relevant agreements signed under it [Title & No], with the ECCC ('the agreements') for the Call for expression of interest for the deployment and operation of cross-border SOC platforms

hereby:

1. Mandate

[full official name of the coordinator] *[ACRONYM]*

[*official legal status or form*]

[*official registration No*][27]

[full official address]

[*VAT number*],

represented by [forename, surname and function of the legal representative of the coordinator] ('the coordinator')

[25] To be deleted or filled out in accordance with the 'Legal Entity' form.

[26] To be deleted or filled out in accordance with the 'Legal Entity' form.

[27] To be deleted or filled out in accordance with the 'Legal Entity' form.

to sign in my name and on my behalf the agreements and their possible subsequent amendments with the ECCC.

2. Mandate the coordinator to act on behalf of the partner in compliance with the agreements. I hereby confirm that the partner accepts all terms and conditions of the agreements and, in particular, all provisions affecting the coordinator and the other partners.

I hereby accept that the partner will do everything in its power to help the coordinator fulfil its obligations under the agreements, and in particular, to provide to the coordinator, on its request, whatever documents or information may be required.

I hereby declare that the partner agrees that the provisions of the agreements, including this mandate, take precedence over any other agreement between the partner and the coordinator which may have an effect on the implementation of the agreements.

This mandate is annexed to the Call for expression of Interest and Hosting and Usage Agreement and forms an integral part of it.

3. Commit to transfer to the Coordinator in a timely manner my share of the remaining acquisition costs of the tools and infrastructures which will not be covered by the Union's financial contribution.

I hereby confirm that I have agreed in writing with the other participating National SOCs in my consortium the amount I will transfer to the Coordinator as a share of said remaining acquisition costs.

Herewith I enclose evidence of this commitment in the form of a letter of commitment signed by the appropriate parties.

SIGNATURE

[forename, surname, function of the legal representative of the mandating partner]

[signature]

Done at [place], [date]

In duplicate[28] in English]

[28] Original mandate and commitment letters to be submitted with the application and annexed to the agreement – second original to be kept by the coordinator.

Annex 5. Blueprint Architecture

This annex aims at setting a blueprint architecture for this initiative. It should not be meant as mandatory top-down implementation guide, but as an effort to harmonise jargon, functionalities and approaches.

For the purpose of this proposal, it is considered that many SOCs and cybersecurity networks or teams are already in place in the MSs, and that each MS organises its own network of SOCs as it wishes. Therefore, for the purpose of this document each MS is a black box. In the end, it is only expected that each MS should designate a single point of contact that would interact with the rest of the network: the MS's national SOC.

This annex is organised as follows. Section 2 details the building blocks composing a national SOC. Section 3 presents the general overview of the EU network of SOCs. Finally, Section 4 details the functionalities of the network.

1. Building blocks of a national SOC

A national SOC can be defined as a centralised security organisation that assists companies and organisations of a MS in identifying, managing, and remediating distributed security attacks.

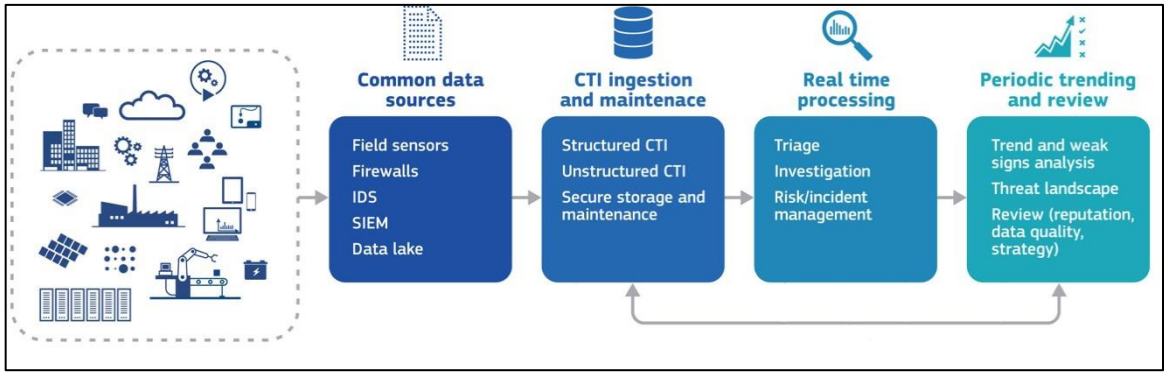

Figure 1. Building blocks of a national SOC.

From a functional point of view (Figure 1), it is generally composed of four building blocks:

- common data sources (public or private sector, such as national CSIRTs, vendor products, self-made internal IT systems or companies, social media and (dark) web, sectorial CERTs or Information Sharing and Analysis Centres (ISACs).
- CTI ingestion and maintenance: to remodel unstructured collected data into structured ones and help the SOC to assimilate the collected data correctly and to build a clean data set of CTI.
- real time processing (to detect anomalies, correlate events etc.)
- periodic trending and review (to assess the quality of the data collected, identify high-level trends or global threats).

These elements do not need to be all present in a national SOC at the moment of the launch of this initiative, however, they can be understood as the functionalities which every SOC should tend to have in the long run.

2. General overview of possible cross-border architectures

As highlighted in the previous section, every MS is free to organise its internal network of SOCs as it wishes: the architecture of the national networks of SOCs is a black box from the point of view of the EU network of SOCs. Each MS participating to this EU network should designate a **national SOC** that will act as a proxy between its

own national network and the rest of the EU network, and in case, also as coordinator which will partake in a joint procurement foreseen by this initiative.

The participating MSs can be grouped by **consortium** that may, for instance, cover specific geographical areas of the EU, and provide CTI to relevant entities in their area of operation. Each consortium must develop a **cross-border SOC platform** to allow the national SOCs of its participating MSs to communicate together and disseminate their collected information via sharing and reporting CTI or cybersecurity incidents.

The various consortia are then interconnected together via a dedicated cross-border **gateway** in order to share their aggregated CTI or cybersecurity incidents. They would form the EU network of SOCs.

This section presents the two architectural layers of the network:

- The *lower layer*, at the level of the consortia (how the MSs of the consortium are organised among themselves),
- The *upper layer*, at the level of the EU network of SOCs (how the interoperability and sharing is guaranteed among the various consortia participating to the network).

2.1. Topological structure of the lower layer

The topological structure of a consortium interconnecting different MSs (each MS having its own national SOC) can be essentially of three types, namely centralised, decentralised or fully distributed. Figure 2 depicts these three topologies.

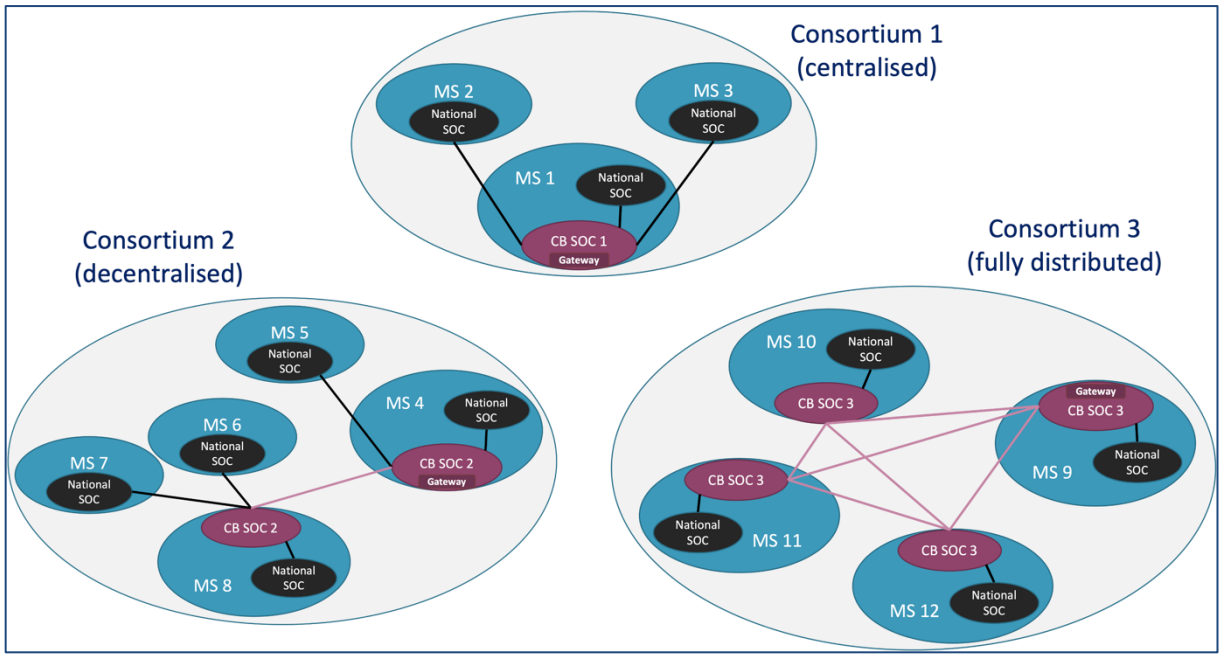

Figure 2. Different topologies of architecture for consortia.

In a **centralised** architecture, data and operations are at a central location. A designated MS hosts the entire cross-border SOC platform and gateway to collected and share the CTI of the consortium with the rest of the network.

In a **decentralised** architecture, few core or "central" nodes (geographically distributed) share information directly among themselves and they are surrounded by their local satellite nodes.

Finally, in a **fully distributed** architecture, a consortium is similar to a full peer-to-peer network where each MS hosts a part of the cross-border SOC platform in order to communicates with all the others. As for the other topologies, one designated MS also hosts the gateway to collected and share the CTI of the consortium with the rest of the network.

The long-term goal of this initiative is to ensure that information flows not only among entities of the same consortia, but also across different consortia.

2.2. Topological structure of the upper layer

The topological structure of the proposed EU network of SOCs interconnecting different cross-border SOC gateways (each consortium having one gateway) can be essentially of two types: centralised or fully distributed. Figure 3 depicts these two topologies.

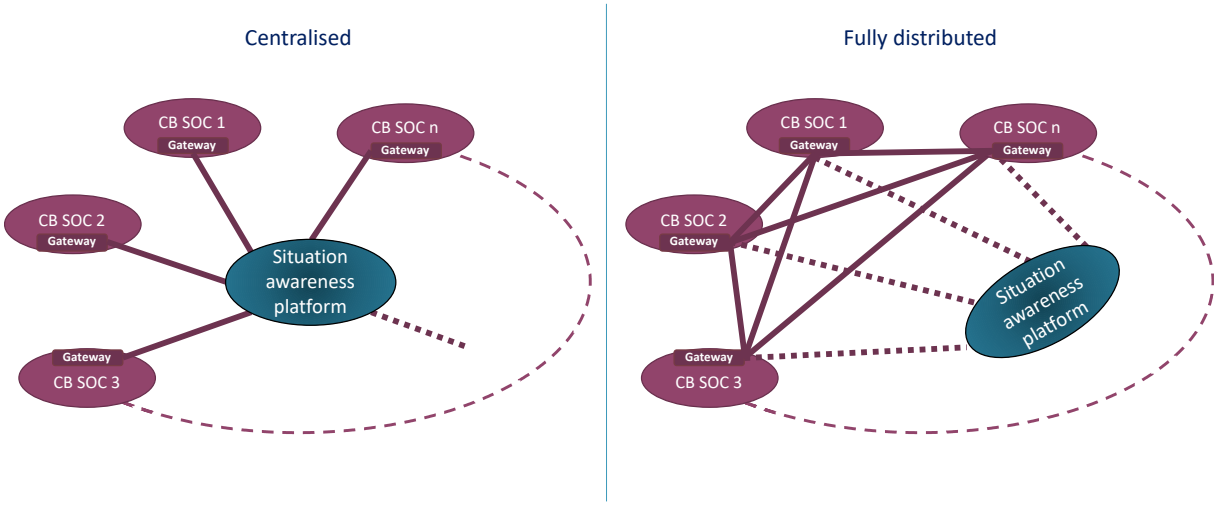

Figure 3. High level view of the different topologies of architecture the EU network of SOCs.

3. Functionalities of the network

The proposed EU network of SOCs must put in place a certain number of mandatory functionalities in order to provide the best results possible in terms of cybersecurity. This section details these mandatory functionalities: sharing, aggregation, correlation, reporting, dashboard crowding, and security.

Figure 4 provides a complete overview of the network with the centralised topology[29]. It further highlights the location of the functionalities within the network (i.e., which component must implement which functionality). Note that the “security" functionality must be implemented everywhere in the network, and therefore it is not depicted in the figure.

[29] The figure of the network with the fully decentralised topology is the same figure without the situation awareness platform.

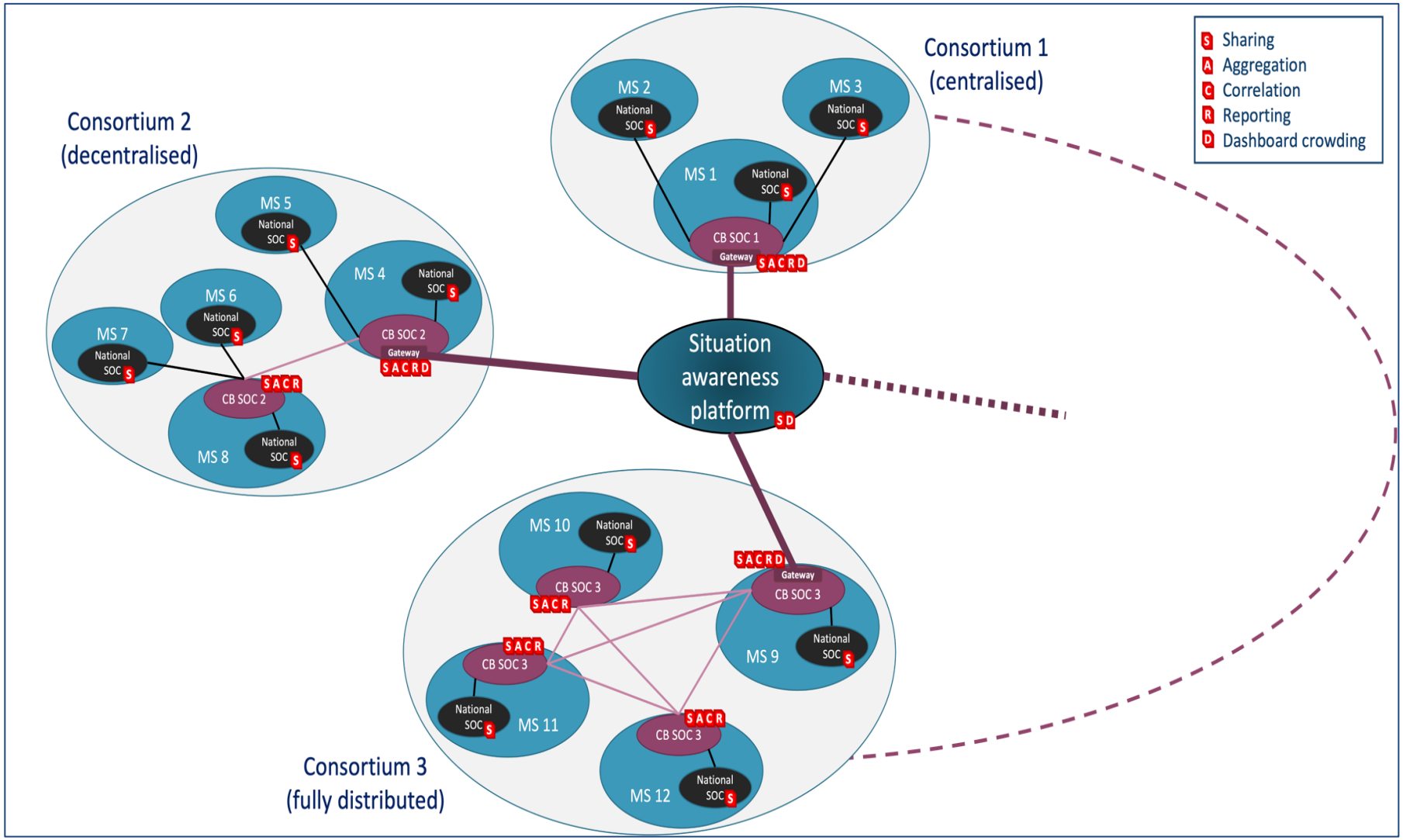
Consortium 1
(centralised)
Consortium 2
(decentralised)
Consortium 3
(fully distributed)
S Sharing
A Aggregation
C Correlation
R Reporting
D Dashboard crowding
MS 1
MS 2
MS 3
MS 4
MS 5
MS 6
MS 7
MS 8
MS 9
MS 10
MS 11
MS 12
National SOC
CB SOC 1
CB SOC 2
CB SOC 3
Gateway
S A C R D
S A C R
Situation awareness platform
S D

Figure 4. Full overview of the proposed EU network of SOCs with the mandatory functionalities.

4. Security

As the network will share potentially sensitive information, security of the data at rest and in transit is paramount.

In all the various network architectures described previously, it is necessary to define common security requirements. The different national SOCs need to exchange data with each other, meaning that they should be able to put in place bidirectional communication. With a centralised topology, there would be a main central cross-border SOC platform collecting information, but this information could be redistributed to regular nodes which should therefore be able to both send and receive data in a secure manner. This is even clearer in case of decentralised or fully distributed topology. SOCs need to act both as client and server for information exchange. Figure 5 gives an overview of the high-level fully distributed architecture interconnecting three SOCs of three different MSs.

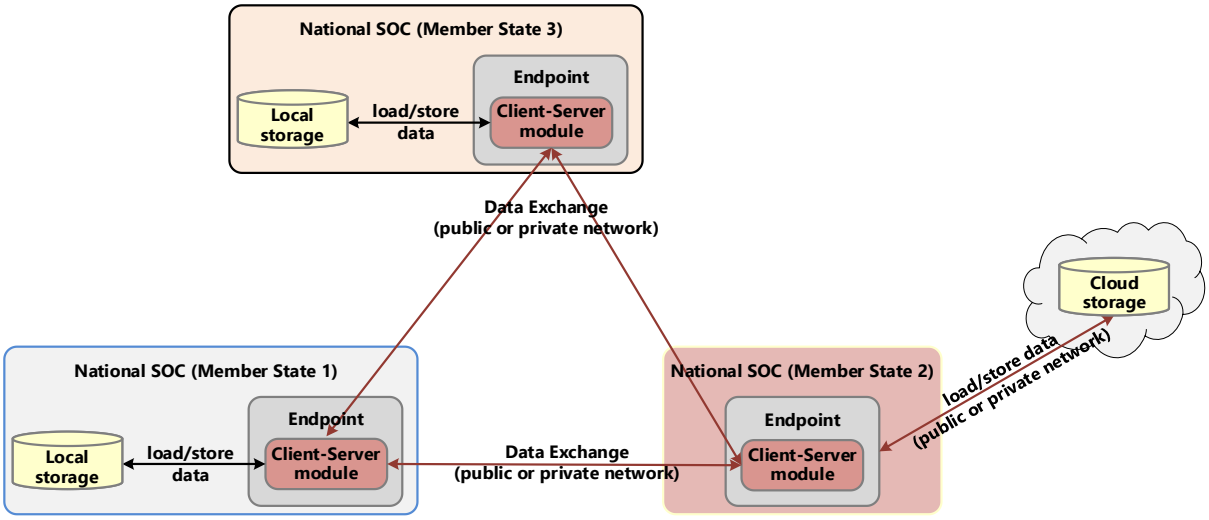

Figure 5. High level architecture for SOCs interconnection

4.1. Security of networks and communications

Exchange of data between two endpoints of two different national SOCs needs to be secured. The communication can take place over unsecure channels (e.g., the Internet), so it is fundamental to apply security measures at different layers of the Open Systems Interconnection (OSI) model[30]. An alternative to public networks could be the use of the current version of the Trans European Services for Telematics between Administrations (TESTA-ng), which already interconnects some public administrations and offers security features.

Protection of communications should rely at least on Transport Layer Security (TLS) protocol and on asymmetric cryptography. With asymmetric encryption, each endpoint would be responsible for the security of its private key, which should be stored in a tamper-proof device such as a Hardware Security Module (HSM) or a smart card.

The measure above however does not guarantee confidentiality of network interactions, i.e., information that could be revealed at the network layer of the OSI model for example by the IP packet headers (e.g., type of transport protocol, addresses). A solution for this could be the realization of a site-to-site Virtual Private Network (VPN) between the different network gateways in the national nodes, for example leveraging on the Internet Protocol Security (IPSec) suite of protocols to implement network tunnelling.

A supplementary measure could be the choice of implementing application layer encryption, thus providing end-to-end security at the highest point of the network stack, i.e., at user level.

[30] Standard ISO/IEC 7498.

4.2. Security of data-at-rest

Data should not be kept in plain in the data storages. Data storages should be encrypted with the state-of-the-art algorithms, and encryption keys protected and managed using tamper-proof devices. The encryption could be implemented by the application sharing data with the others, left to specific features of the database software, or realised through disk encryption functionalities. In all the cases above, it must be highlighted that storage encryption can introduce performance reduction and additional management overhead, for example when nodes reboot. Therefore, due care is necessary when selecting the solution according to the specific scenario and context.

4.3. Credentials management

Previous sections mention the use of digital certificates and of public and private keys in the context of asymmetric cryptography. Creation, distribution, and management of these electronic credentials need to be assigned to a Public Key Infrastructure (PKI), and therefore to a Certificate Authority (CA) issuing the digital certificates. The strengths and reliability of the PKI is of utmost importance, with possibility to rely on public or private PKIs

A crucial step in the issuance is the identification of the entities that have access to the system and secure delivery of credentials to them. As already said, each entity should generate its own key pair and a request to sign its certificates. The pair should be generated directly on a smartcard or HSM so that the private key never leaves the tamper-proof device. The public key extracted to generate the certificate that would be signed using the CA's root private key. The latter is a crucial aspect whose protection again should be entrusted to an HSM device. It is important that deliveries of certificates to a user are done with no intermediaries, and that the support (typically the smartcard) is protected by an authentication factor (e.g., a PIN) which is delivered through another channel and always kept separately from the support itself. Secure architecture

The introduction of the security measures described in the previous sections, brings to a refinement and enrichment of the high-level architecture depicted in Figure 5. Those changes reflect the presence of the different security components, such as digital certificates, key pairs, and gateways for network traffic encryption. This brings to a secure architecture shown in, that indeed puts in place both TLS and VPN encryption for two layers of protection in the exchange of data.

Figure 6 provides an example of the integration of all the elements described in this section.

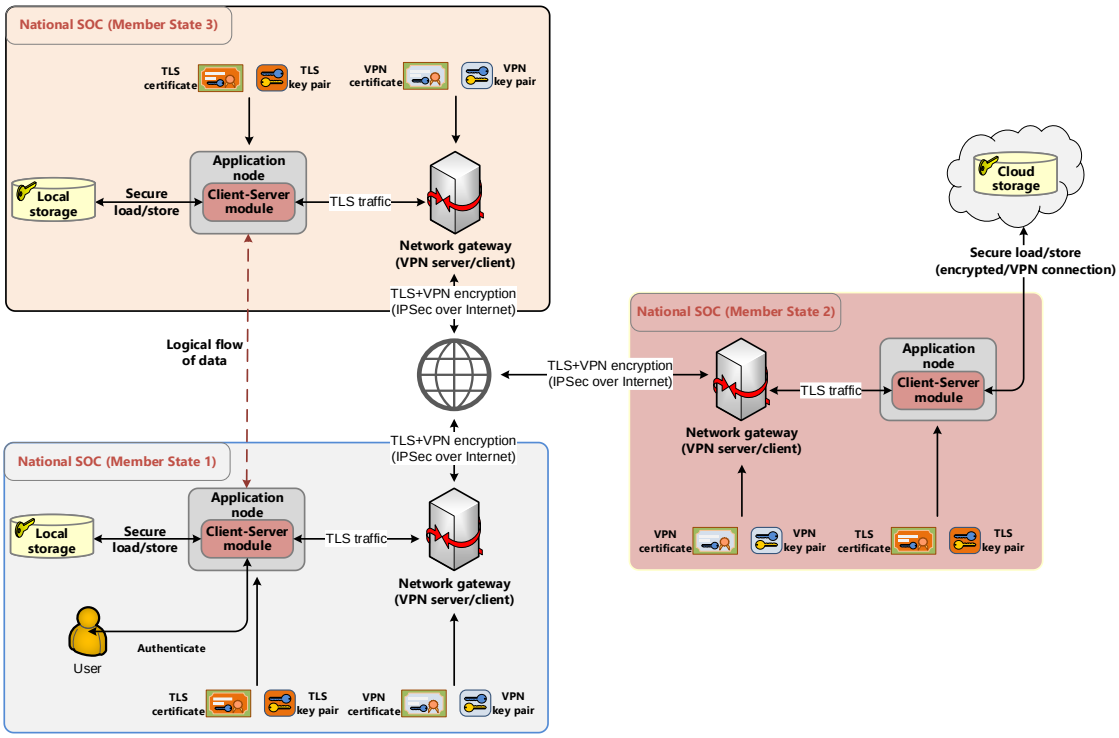

Figure 6. Secure architecture for SOCs interconnection.

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**
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**