Digital Europe Programme (DIGITAL)

Call for proposals

Deployment Actions in the area of Cybersecurity
(DIGITAL–ECCC–2024–DEPLOY–CYBER–07)

Version 3.0
6 January 2025

HISTORY OF CHANGES				
Version	**Publication Date**	**Change**		**Page**
1.0	04.06.2024	▪ Initial version		
2.0	11.06.2024	▪ Deadline date correction		43
2.1	19.07.2024	▪ Cost eligibility rules correction (section 10)		36
3.0	06.01.2025	▪ Deadline date correction		

EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

CNECT.H– Digital Society, Trust and Cybersecurity CNECT.H.1
Cybersecurity Technology and Capacity Building

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction

This is a call for proposals for EU **action grants** in the field of Cybersecurity under the Digital Europe Programme (DIGITAL).

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2018/1046 (EU Financial Regulation)
- the basic act (Digital Europe Regulation 2021/694[1]).

The call is launched in accordance with the 2023-2024 Work Programme[2] and will be managed by the **European Commission, Directorate-General for Communication, Networks, Content and Technology (DG CONNECT), on behalf of the European Cybersecurity Competence Centre (ECCC), until the ECCC has the capacity to implement its own budget.**

The call covers the following **topics**:

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs**

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms**

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS - Strengthening the SOC Ecosystem**

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies**

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations**

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call Document, the Model Grant Agreement, the EU Funding & Tenders Portal Online Manual and the EU Grants AGA — Annotated Grant Agreement.

These documents provide clarifications and answers to questions you may have when preparing your application:

- the Call Document outlines the:

  - background, objectives, scope, outcomes and deliverables, KPIs to measure outcomes and deliverables, targeted stakeholders, type of action and funding rate and specific topic conditions (sections 1 and 2)

---

[1] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme (OJ L 166, 11.5.2021, p. 1).

[2] Commission Implementing Decision C(2023) 8620 final of 14.12.2023 concerning the adoption of the work programme for 2023-2024 and the financing decision for the implementation of the Digital Europe Programme.

- timetable and available budget (sections 3 and 4)

- admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)

- criteria for financial and operational capacity and exclusion (section 7)

- evaluation and award procedure (section 8)

- award criteria (section 9)

- legal and financial set-up of the Grant Agreements (section 10)

- how to submit an application (section 11).

- the Online Manual outlines the:

  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')

  - recommendations for the preparation of the application.

- the AGA — Annotated Grant Agreement contains:

  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc.)*

1. Background

Digital technologies are profoundly changing our daily life, our way of working and doing business, the way we understand and use our natural resources and environment and the way we interact, communicate and educate ourselves. The critical role of digital technologies and infrastructures, and the interdependencies in our societies and economies, have recently been demonstrated by disruptive events such as the COVID- 19 crisis and Russia's war of aggression against Ukraine. These crises have confirmed how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world. Malicious cyber activities not only threaten our economies but also our way of life, our freedoms and values and even try to undermine the cohesion and functioning of our democracy in Europe. The second Work Programme (WP) Cybersecurity of the Digital Europe Programme 2023-2024 introduces actions that further develop the EU's cybersecurity capabilities and enhance its resilience in the context of the EU Cybersecurity Strategy.

Actions included in this call document will in particular support the objectives indicated below.

- Actions in order to create an advanced (state of the art) threat detection and cyber incident analysis ecosystem by building capacities of Security Operation Centres (SOCs), at National and Cross-Border levels. These are actions in support of the European Cyber Alert System building up as defined in the Cyber Solidarity Act.

- Actions targeting at strengthening the existing SOC Ecosystem.

- Actions that aim at developing breakthroughs in Key Digital Technologies such as Artificial Intelligence (including generative AI and adversarial AI), Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking, with the objective of enabling European cybersecurity actors to take advantage of them by improving detection and prevention capabilities, efficiency, scalability, and facilitating data sharing and regulatory compliance.

- A mechanism that aims to complement efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures.

- Actions that focus on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislations on cybersecurity.

- All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation.

2. Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action and funding rate — Specific topic conditions

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs

National SOCs are public entities given the role at national level to act as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting Cyber Threat Intelligence (CTI), reviews and analyses. They provide a central operational capacity and support other SOCs at national level (e.g., by offering guidance or training, making available data or analysis of this data, coordinating joint detection and monitoring actions). They will play a central role at national level and can act as a hub within a context of SOCs in the different countries.

Objectives

The objective is to create or strengthen National SOCs, in particular with state-of-the- art tools for monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs. They will also, where possible, benefit from information and feeds from other SOCs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis.

Scope

The aim is capacity building for new or existing National SOCs, e.g., equipment, tools, data feeds, as well as costs related to data analysis, interconnection with Cross-Border SOC platforms, etc. This can include for example automation, analysis and correlation tools and data feeds covering Cyber Threat Intelligence (CTI) at various levels ranging from field data to Security Information and Event Management (SIEM) data to higher level CTI. National SOCs should also leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context.

This also includes the use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information. The operations should be built upon live network data. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

A key element is the translation of advanced AI/ML, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real conditions in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms).

Another key role for National SOCs is knowledge transfer, such as training of cybersecurity

analysts. For example, SOCs dealing with critical infrastructures play a key role and should benefit from the knowledge and experience acquired by or concentrated in National SOCs.

National SOCs must share information with other stakeholders in a mutually beneficial exchange of information and commit to apply to participate in a cross-border SOC platform within the next 2 years, with a view to exchanging information with other National SOCs.

To achieve this aim, a call for expression of interest[3] will be launched to select entities in Member States that provide the necessary facilities to host and operate National SOCs. Applicants to the call for expressions of interest should describe the aims and objectives of the National SOC, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the National SOC, the services it will offer, the way they will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the National SOC, its services and its infrastructure.

To support the above activities of a National SOC, the following two workstreams of activities are foreseen:

a) [Procurement][4] A Joint Procurement Action with the Member State where the national SOC is located: this will cover the procurement of the main equipment, tools and services needed to build up the National SOC

b) [Building up and running the National SOC] A grant will also be available to cover, among others, the preparatory activities for setting up the National SOC, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National SOC, e.g. using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

These actions aim at creating or strengthening national SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services.

SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

---

[3] Please note this is not a call for expression of interest within the meaning of Point 13 of Annex I of the Regulation (EU, Euratom) 2018/1046. The aim is to select the future contracting authorities taking part in a joint procurement.

[4] For the topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC and DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT an expression of interest shall also be submitted no later than the 27 March 2025 at 17:00 Brussels time. Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en. Applications must be submitted in the correct form, duly completed and dated. They must be submitted in electronic copy on https://cybersecurity-centre.europa.eu/funding-opportunities_en and signed by the person authorised to enter into legally binding commitments on behalf of the applicant organisation. The electronic version must contain the pdf versions of the application and other files as described in the call for expression of interest.

Outcomes and deliverables

- World-class National SOCs across the Union, strengthened with state-of-the-art technology, acting as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.

- Threat intelligence and situational awareness capabilities and capacity building supporting strengthened collaboration between cybersecurity actors, including private and public actors.

KPIs to measure outcomes and deliverables

- Maturity analysis pre and post implementation to measure the change in capacity of the beneficiary(ies).

- Number of entities benefitting from the SOCs operations.

- Intensity of exchange of information between funded entities.

- Cyberthreat intelligence and situational awareness services developed.

Targeted stakeholders

The target stakeholders under a) and b) above are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU". Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

Type of action and funding rate

Simple Grants — 50% funding rate

ℹ For more information on Digital Europe types of action, *see Annex 1.*

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*

- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*

- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

  - extent to which the project would reinforce and secure the digital technology supply chain in the Union

  - extent to which the proposal can overcome financial obstacles such as the lack of market finance

  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT — Enlarging existing or Launching New Cross-Border SOC Platforms

Objectives

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.

This action aims at new cross-border SOC platforms, as well as supporting those that were already launched under the previous DIGITAL work programme (2021-2022). While the main focus of this action is on processes and tools for prevention, detection and analysis of emerging cyber-attacks, it also foresees in particular the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU.

Scope

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 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).

Also, for cross-border SOC platforms, there is a crucial need for novel tools based on advanced Artificial Intelligence and machine learning (AI/ML), data analytics and other relevant cybersecurity relevant technologies, based on research results and further tested and validated in real conditions, in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms).

The platforms will support common situational awareness and effective crisis management and response by providing relevant information to networks and entities responsible for cybersecurity operational cooperation and crisis management at Union level, without undue delay, where they obtain information related to an ongoing large- scale, cross-border incident, or to a major threat or a major vulnerability likely to have significant cross-border impacts or significant impacts on services and activities falling within the scope of the Directive (EU) 2022/2555.

A call for expression of interest[5] will be launched to select entities in Member States that provide the necessary facilities to host and operate Cross-Border SOC platforms for pooling data on cybersecurity threat between several Member States. Applicants to the call for expressions of interest should describe the aims and objectives of the Cross- Border SOC platform, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the Cross-Border SOC platform, the services it will offer, the way they will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the Cross-Border SOC platform, its services and its infrastructure.

---

[5]   Please note this is not a call for expression of interest within the meaning of Point 13 of Annex I of the Regulation (EU, Euratom) 2018/1046. The aim is to select the future contracting authorities taking part in a joint procurement.

To support the above activities of a Cross-Border SOC platform, the following two workstreams of activities are foreseen:

a)   [Procurement][6] A Joint Procurement Action with the Member State participating in the Cross-Border SOC platform: this will cover the procurement of the main equipment, tools and services needed to build up the Cross-Border SOC platform.

b)   [Building up and running the Cross-Border SOC platform] A grant will also be available to cover, among others, the preparatory activities for setting up the Cross- Border SOC platform, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Cross- Border SOC platform, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

These actions aim at creating or strengthening cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

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

Outcomes and deliverables

* World-class cross-border SOC platforms across the Union for pooling data on cybersecurity threat between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.
* Sharing of Threat Intelligence between National SOCs, and information sharing agreements with competent authorities and CSIRTs.

KPIs to measure outcomes and deliverables

* Maturity analysis pre and post implementation to measure the change in capacity of the beneficiary(ies).

---

[6]   For the topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC and DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT an expression of interest shall also be submitted no later than the 27 March 2025 at 17:00 Brussels time. Application forms will be available on https://cybersecurity-centre.europa.eu/funding-opportunities_en. Applications must be submitted in the correct form, duly completed and dated. They must be submitted in electronic copy on https://cybersecurity- centre.europa.eu/funding-opportunities_en and signed by the person authorised to enter into legally binding commitments on behalf of the applicant organisation. The electronic version must contain the pdf versions of the application and other files as described in the call for expression of interest.

- Number of entities benefitting from the SOCs operations.

- Intensity of exchange of information between funded entities.

- Cyberthreat intelligence and situational awareness services developed.

Targeted stakeholders

The target stakeholders under a) and b) above are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU". Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

Type of action and funding rate

Simple Grants — 50% funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*

- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*

- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

    - extent to which the project would reinforce and secure the digital technology supply chain in the Union

    - extent to which the proposal can overcome financial obstacles such as the lack of market finance

    - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS — Strengthening the SOC Ecosystem

Objectives

This topic complements other actions in this and the previous Work Programme, which are building up National SOCs and Cross-Border SOC platforms. It will empower SOCs which are linked to National SOCs, and to a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms, leading to an increased data sharing and better detection capability for cyber threats. This should in particular foster interoperability, identifying what data can be shared, how this is shared and in what format, requirements and sharing agreements, and ways to enable better exchange.

Links to the actions funded under the Cybersecurity Skills Academy (in the main Digital Europe work programme) can also be envisaged.

These actions should lead to increased engagement, including from the private sector, and to a better collaboration towards a common EU cyber threat knowledge base and technological independence.

Additionally, Cross-Border SOC Platforms will develop a comprehensive governance framework, with for example enrolment conditions and vetting procedures. The aim is to foster discussion between such platforms, sharing best practices and identifying opportunities for collaboration. One Coordination and support action will be selected, bringing together the largest possible network of National and Cross-Border SOC platforms.

Scope

Actions should address one or more of the following:

- Activities and technical frameworks that foster the collaboration and interconnection between Cross-Border SOC platforms and National SOCs, as well as fostering the link between National SOCs and other SOCs at national level.

- Actions that support the cooperation and coordination of Cross-Border SOC platforms, both between different Cross-Border SOC platforms, and with relation to national SOCs and other SOCs.

- Actions to foster links between public sector and industry, and stimulate mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities.

- Actions to foster links between SOCs and industrial stakeholders in artificial intelligence and in other enabling technologies, fostering the adoption of such technologies, including AI techniques and tools rand facilitating getting acquainted with existing state of the art tools (such as for example those developed in Action 1.1.4 of this work programme) and knowledge exchange.

- Actions to engage stakeholders from the HPC stakeholder community and practitioners of breakthrough AI technologies, to develop a blueprint for the requirements of AI models that necessitate access to large or smaller HPC facilities, and next steps to make this happen, as well as raising awareness of this in the wider SOC community.

These actions aim at creating or strengthening national and/or cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU)2021/694.

Indicatively one proposal is expected to be financed via this topic.

In accordance with the Cyber Solidarity Act (to be adopted and publish in the Official Journal in autumn 2024), ENISA is tasked to develop guidelines on the interoperability of Cross-Border Cyber Hubs. Against this background, the selected proposal shall be required to collaborate with ENISA on the aspect of the interoperability.

Outcomes and deliverables

- Events, workshops, stakeholder consultations, architectural designs and white papers on technical coordination and interconnection support platforms.

- Stronger links between public sector and industry SOCs

- Technical frameworks to allow for information exchange between SOC platforms

- A blueprint for the use of HPC facilities for the benefit of SOCs

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- *Number of events, workshops, stakeholder consultations, and white papers to fostering the development of the SOCs ecosystem.*

- *Number of awareness raising, dissemination and other stakeholder engagement activities.*

- *Number of active collaborations implemented with other relevant initiatives or European players and projects.*

Targeted stakeholders

National SOCs, Cross-Border SOC Platforms and other relevant stakeholders.

Type of action and funding rate

Coordination and Support Actions — 100% funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)

- For this topic, following reimbursement option for equipment costs applies: depreciation only (see section 10)

- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

    - extent to which the project would reinforce and secure the digital technology supply chain in the Union

    - extent to which the proposal can overcome financial obstacles such as the lack of market finance

    - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies

Objectives

Breakthroughs in Key Digital Technologies such as Artificial Intelligence (including generative AI and adversarial AI), Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking, create new opportunities for advancing cybersecurity in the areas of vulnerability detection, threat detection and rapid response, reducing the window of opportunity for attackers to exploit these vulnerabilities. Furthermore, they may enable new possibilities to protect data security and privacy.

The objective is to enable European cybersecurity actors to take advantage of these new breakthroughs, improving detection and prevention capabilities, efficiency, scalability, and facilitating data sharing and regulatory compliance.

In particular innovative technologies should allow for the processing of larger amounts of data, automating real-time pattern recognition, log analysis, vulnerability scanning, while enabling security professionals to focus on higher level interpretation of data and response decisions. They should allow organisations to deploy solutions and larger scale, and in increasingly complex environments.

A priority is to create and strengthen capacity for original Cyber Threat Information (CTI), e.g., in the form of CTI feeds or services.

Scope

Activities should fortify cybersecurity capabilities using breakthrough technologies, encompassing various aspects of cybersecurity. This involves uptake and integration for the deployment of novel tools, systems and services for threat detection, incident response, malware defence, vulnerability management, data protection and so forth. In one or more of the following topics should be addressed:

- Real-time Monitoring and Incident Response: ensuring the swift identification and response to security incidents through continuous network monitoring, alert generation, and automated response mechanisms.

- Malware Defence and Analysis: mitigating malware threats by analysing code behaviour, scrutinizing network traffic, and assessing file characteristics, thereby reducing opportunities for attackers to exploit vulnerabilities.

- Proactive Vulnerability Management: identifying and addressing weaknesses proactively through automated vulnerability scanning and penetration testing to address potential threats before they can be exploited.

- Data Protection and Anomaly Detection: safeguarding sensitive data by scrutinizing access patterns and identifying abnormal behaviour to mitigate data breaches and protect critical information.

- Incident investigation to help uncover cause, scope and impact of security incidents or breaches that have occurred.

- Data Utilisation with Privacy: enabling organisations to harness data for analysis and insights while preserving data security and privacy through techniques such as anonymisation and de-identification.

By addressing such issues, the cybersecurity resilience of organisations should be enhanced, improving overall cybersecurity posture, encompassing various aspects such as threat detection,

16

incident response, and vulnerability management.

In well justified cases, access requests to the EuroHPC high performance computing infrastructure could be granted.

The systems, tools and services developed under this topic, where relevant, will be made available for licencing to National and/or Cross-Border SOC platforms under favourable market conditions.

This action aims at the deployment of key technologies in cybersecurity, in particular also in the context of securing national authorities, providers of critical infrastructures and essential services. As this involves the handling of cyber incidents, malware and management of vulnerabilities that could be exploited by malicious actors, the deployment of such technologies must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.

As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- Deployment of state-of-the-art technologies in the area of cybersecurity

- Tools for automated threat detection, monitoring of networks, data protection and incident response

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- *Number of entities benefitting from project activities.*

- *Number of cybersecurity new* technologies deployed in operational environments.

- *Number of* tools for automated threat detection and incident response.

- *Number of o*riginal Cyber Threat Information (CTI) feeds created and deployed in operational environment*.*

Targeted stakeholders

The target stakeholders are technology companies, especially SMEs, working to provide and support other private and public organisations with cyber threat detection and CTI feeds.

Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

Type of action and funding rate

SME Support Actions — 50% and 75% (for SMEs) funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

− For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*

− For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*

− The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

− extent to which the proposal can overcome financial obstacles such as the lack of market finance*

− extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

Objectives

This mechanism aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Scope

The provision of preparedness support services (ex-ante) shall include activities listed below, addressing for example large industrial installations or infrastructures, operators of essential services, digital service providers and governmental entities:

Support for testing for potential vulnerabilities:

• Development of penetration testing scenarios. The proposed scenarios may cover Networks, Applications, Virtualisation solutions, Cloud solutions, Industrial Control systems, and IoT.

• Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.

• Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.

• Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).

• Consulting services, providing recommendations on how to improve infrastructure security and capabilities.

Support for threat assessment and risk assessment:

• Threat Assessment process implementation and life cycle

- Customised risk scenarios analysis.

Risk monitoring service:

- Specific continuous risk monitoring such as attack surface monitoring, risk monitoring of assets and vulnerabilities.

Preparedness actions should benefit entities (including SMEs and start-ups) in sectors indicated as critical infrastructure sectors in NIS2 (Directive (EU) 2022/2555), such as energy, transport and banking, and entities in other relevant sectors.

This action aims at the creation of platforms that serve as a reference point and provide services such as penetration testing and threat assessments for providers of essential services and critical infrastructures, as well as other actors. This involves data and operational measure regarding cybersecurity, including penetration tests and exploitable vulnerabilities. Such information could be exploited by malicious actors, and thus it must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk.

Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Outcomes and deliverables

- preparedness support services

- threat assessment and risk assessment services

- risk monitoring services

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance.

Proposals may include the indicators listed below or those of their choice. When applicable, baseline and target values must be provided.

- *number of penetration tests provided*

- *number of essential entities supported*

- *number of threat assessments / risk scenario analyses carried out*

- *number of risk monitoring services provided*

- *number of potential users covered per test/exercise*

- *number and nature of vulnerabilities discovered*

- *number of cross-border actions/exercises*

Targeted stakeholders

This topic targets in particular industrial players, national cybersecurity authorities, national

cybersecurity competence centres, National Coordination Centres (as defined in Regulation (EU) 2021/887), private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries, to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties.

Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

Type of action and funding rate

Grants for Financial Support — 100% funding rate

For more information on Digital Europe types of action, *see Annex 1.*

Specific topic conditions

− For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*

− For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*

− For this topic, financial support to third parties is compulsory *(see section 10)*

− The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

  − extent to which the proposal can overcome financial obstacles such as the lack of market finance*

  − extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

Objectives

The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555)[7], the Cybersecurity Act [8], and the Directive on attacks against information systems (Directive 2013/40) [9]. It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous Digital Work Programme.

In addition, this action also aims at supporting the implementation of the proposed Cyber Resilience Act (CRA) [10] by market surveillance authorities/notifying authorities/national accreditation bodies, by increasing their capacities to ensure effective implementation of the CRA.

---

[7]   See https://eur-lex.europa.eu/eli/dir/2022/2555

[8]   See https://eur-lex.europa.eu/eli/reg/2019/881/oj

[9]   See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

[10] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

Proposals should contribute to achieving at least one of these objectives:

- Development of trust and confidence between Member States.

- Supporting market surveillance authorities/notifying authorities/national accreditation bodies to implement the CRA.

- Effective operational cooperation of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services including public authorities.

- Better security and notification processes and means for Essential and Important Entities in the EU, including cross-border (automated) incident notification systems.

- Better reporting of cyber-attacks to law enforcement authorities in line with the Directive on attacks against information systems.

- Improved security of network and information systems in the EU.

- More alignment of Member States' implementations of NIS2 (Directive (EU) 2022/2555).

- Support cybersecurity certification in line with the amended Cybersecurity Act.

Scope

The action will focus on the support of at least one of the following priorities:

- Implementation, validation, piloting and deployment of technologies, tools and IT- based solutions, processes and methods for monitoring and handling cybersecurity incidents.

- Increasing capacity for market surveillance authorities/notifying authorities/national accreditation bodies in view of tasks as provided by the CRA.

- Collaboration, communication, awareness-raising activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).

- Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.

- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.

- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.

- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.

- Enhance the transparency of security properties of products with digital elements.

- Enable businesses across all sectors and consumers to use products with digital elements securely.

- Support to Cybersecurity certification, including support to national cybersecurity certification authorities and other relevant stakeholders, such as SMEs. This includes activities such as threat-led penetration testing, acquiring certification testbeds, sharing best practices,

implementing innovative evaluation methods for specific ICT products or components.

Proposals may target, where relevant, Member State competent authorities, which play a central role in the implementation of NIS2 (Directive (EU) 2022/2555), as well as other actors within the scope of this Directive.

Proposals may support, amongst others, the continuation of cybersecurity activities funded through the CEF Telecom programme, building where relevant on the results from the CEF projects.

Proposals may support, amongst others, for the onboarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555) and are potential contributors to the goals of the CEF Cybersecurity Core Service Platform.

Outcomes and deliverables

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.

- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.

- Organisation of events, workshops, stakeholder consultations and white papers.

- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.

- Support actions and cooperation for further advanced of cybersecurity certification.

- Effective supervision and enforcement of the CRA by the market surveillance authorities and adequate capabilities of notifying authorities and national accreditation bodies for the implementation of the CRA.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of technologies and IT-based solutions, processes and methods for handling cybersecurity incidents implemented, validated, piloted or deployed.

- Number of activities organised for collaboration, communication, awareness raising or knowledge exchange and training (on the implementation of the NIS2 Directive).

- Number of twinning schemes implemented between at least two Member States for effective cross-border collaboration preventing, detecting and countering cybersecurity incidents.

- Number of tools and IT-based solutions, processes and methods for monitoring and handling exploited vulnerabilities in products with digital elements in the scope of the CRA.

- Number of products or services available that simplify and/or automate CRA compliance.

- Number of SMEs using open access or low-cost tools to support the implementation of the CRA for public authorities and economic operators.

- Number of tools to support market surveillance authorities and notifying authorities appointed under the CRA in the implementation of their respective mandates.

- Number of communications, awareness-raising events, knowledge exchange and training activities about the rules of the CRA.

- Number of activities organised to promote sharing of technical specifications, best practices and use-cases amongst actors that have obligations under the CRA.

- Uptake of CRA compliant products across sectors.

Targeted stakeholders

This topic targets relevant industrial stakeholders, including SMEs and start-ups in the scope of the upcoming CRA, concerned by the NIS2 Directive or that may benefit from the European cybersecurity certification schemes. It refers also to Member State competent authorities, which play a central role in the implementation of the NIS2 Directive, Computer Security Incident Response Teams (CSIRTs) including sectorial CSIRTs, Security Operation Centres (SOC), Operators of Essential Services (OES), digital service providers (DSP), Information Sharing and Analysis Centres- ISACs, actors that play a role in the implementation of the Cyber Resilience Act (including certification bodies), and any other actors within the scope of the legislations mentioned above.

Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

Type of action and funding rate

Simple Grants — 50% funding rate

For more information on Digital Europe types of action, *see Annex 1.*

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*

- For this topic, following reimbursement option for equipment costs applies: depreciation only *(see section 10)*

- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

  - extent to which the proposal can overcome financial obstacles such as the lack of market finance*

  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

3. Available budget

The estimated available call budget is **EUR 102 800 000**.

Specific budget information per topic can be found in the table below:

Topic	Topic budget
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs	**EUR 5.800.000**

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms	**EUR 5.000.000**
DIGITAL-ECCC-2024-DEPLOY- CYBER-07-SOCSYS - Strengthening the SOC Ecosystem	**EUR 2.000.000**
DIGITAL-ECCC-2024-DEPLOY- CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies	**EUR 35.000.000**
DIGITAL-ECCC-2024-DEPLOY- CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations	**EUR 35.000.000**
DIGITAL-ECCC-2024-DEPLOY- CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)	**EUR 20.000.000**

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	4 July 2024
Deadline for submission:	27 March 2025 – 17:00:00 CET (Brussels)
Evaluation:	April - May 2025
Information on evaluation results:	June - July 2025
GA signature:	December 2025

5. Admissibility and documents

Proposals must be submitted before the **call deadline** *(see timetable section 4)*.

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the Search Funding & Tenders section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:

   – Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project *(to be filled in directly online)*
   – Application Form Part B — contains the technical description of the project *(to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded)*
   – **mandatory annexes and supporting documents** *(templates available to be downloaded from the Portal Submission System, completed, assembled and re-uploaded)*:

      – detailed budget table/calculator: not applicable

      – CVs of core project team: not applicable

– activity reports of last year: not applicable

– list of previous projects: not applicable

– **ownership control declarations** (including for associated partners and subcontractors): **applicable**

– **Other annex:** for Topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC the appointment decision from the Member State designating the entity to act as National SOC: **applicable**

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable**, **accessible and printable**.

Proposals are limited to maximum

70 pages (part B) for topics:

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

50 pages (part B) for topic:

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS - Strengthening the SOC Ecosystem

Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents *(for legal entity validation, financial capacity check, bank account validation, etc.)*

For more information about the submission process (including IT aspects), consult the Online Manual.

6. Eligibility

Applications will only be considered eligible if their content corresponds wholly (or at least in part) to the topic description for which they are submitted.

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

– be legal entities (public or private bodies)

- be established in one of the eligible countries, i.e.:
  - EU Member States (including overseas countries and territories (OCTs))
  - EEA countries (Norway, Iceland, Liechtenstein)

Beneficiaries and affiliated entities must register in the Participant Register — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Please be aware that **all topics of this call are subject to restrictions due to security**, therefore entities must not be directly or indirectly controlled from a country that is not an eligible country. **All entities [11] will have to fill in and submit a declaration on ownership and control.**

Moreover:

- participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is limited to entities established in and controlled from eligible countries
- project activities (included subcontracted work) must take place in eligible countries (see section geographic location below and section 10)
- the Grant Agreement may provide for IPR restrictions (see section 10).

Finally, for the topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC and DIGITAL- ECCC-2024-DEPLOY-CYBER-07-SOCPLAT grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

For more information, *see Annex 2.*

Specific cases

Natural persons — Natural persons are NOT eligible (with the exception of self- employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations — International organisations are not eligible, unless they are International organisations of European Interest within the meaning of Article 2 of the Digital Europe Regulation (i.e. international organisations the majority of whose members are Member States or whose headquarters are in a Member State).

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons[12].

EU bodies — EU bodies (with the exception of the European Commission Joint Research Centre) can NOT be part of the consortium.

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[13]. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Countries currently negotiating association agreements — Beneficiaries from countries with

---

[11] Except for entities that are validated as public bodies by the Central Validation Service.

[12] See Article 197(2)(c) EU Financial Regulation 2018/1046.

[13] For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.

ongoing negotiations for participating in the programme *(see list of participating countries above)* may participate in the call and can sign grants if the negotiations are concluded before grant signature and if the association covers the call (i.e. is retroactive and covers both the part of the programme and the year when the call was launched).

EU restrictive measures — Special rules apply for certain entities *(e.g. entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[14])*. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

Following the Council Implementing Decision (EU) 2022/2506, as of 16th December 2022, no legal commitments (including the grant agreement itself as well as subcontracts, purchase contracts, financial support to third parties etc.) can be signed with Hungarian public interest trusts established under Hungarian Act IX of 2021 or any entity they maintain.

Affected entities may continue to apply to calls for proposals. However, in case the Council measures are not lifted, such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties). In this case, co-applicants will be invited to remove or replace that entity and/or to change its status into associated partner. Tasks and budget may be redistributed accordingly.

For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Consortium composition

For the topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs: only entities designated at Member State level as National SOCs are allowed to apply for funding and the project should be mono-beneficiary.

For the topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT consortia shall be composed by beneficiaries from at least 3 eligible countries *in case of new cross-border SOCs.* In case of enlargement of an ongoing cross-border grant, the new consortium should be composed by the coordinator of the ongoing grant plus the new entities that want to join the hosting consortium of the cross-border SOC (see section 6).

For all the other topics: *no restrictions*

Eligible activities

Eligible activities are the ones set out in section 2 above.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

Projects must comply with EU policy interests and priorities *(such as environment, social, security, industrial and trade policy, etc)*.

Financial support to third parties is mandatory in DIGITAL-ECCC-2024-DEPLOY-CYBER- 07-LARGEOPER (Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations) for grants under the following conditions:

---

[14] Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.

- the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality

- the calls must be published on the Funding & Tenders Portal, and on the participants' websites

- the calls must remain open for at least two months

- if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change

- the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries

- the calls must have a clear European dimension.

For other topics, Financial Support to Third Parties is not allowed.

Geographic location (target countries)

Due to restrictions due to security:

- for all topics: the proposals must relate to activities taking place in the eligible countries *(see above)*

Ethics

Projects must comply with:

- highest ethical standards and

- applicable EU, international and national law (including the General Data Protection Regulation 2016/679).

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

For proposals involving development, testing, deployment, use or distribution of AI systems, the ethics review will in particular check compliance with the principles of human agency and oversight, diversity/fairness, transparency and responsible social impact, while the experts performing the technical evaluation will assess the robustness of the AI systems (i.e. their reliability not to cause unintentional harm).

Security

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Decision 2015/444[15] and its implementing rules and/or national rules) provide for instance that:

---

[15] See Commission Decision 2015/444/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded

- classified information must be marked in accordance with the applicable security instructions in the SAL

- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:

    - created or accessed only on premises with facility security clearance (FSC) from the competent national security authority (NSA), in accordance with the national rules

    - handled only in a secured area accredited by the competent NSA

    - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know

- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules

- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)

- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearance may have to be provided before grant signature. The granting authority will assess the need for clearance in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearance.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables *(e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc.)*

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant *(e.g. technology restrictions, national security classification, etc.)* The granting authority must be notified immediately of any potential security issues.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the Participant Register during grant preparation *(e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc.)* The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations

- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information

- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities *(see below, section 10)*

- prefinancing paid in instalments

- (one or more) prefinancing guarantees *(see below, section 10)*

or

- propose no prefinancing

- request that you are replaced or, if needed, reject the entire proposal.

For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the 'Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing

and implementing the project

– description of the consortium participants

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate[16]:

– bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)

– in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)

– guilty of grave professional misconduct[17] (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

– committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

– shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

– guilty of irregularities within the meaning of Article 1(2) of EU Regulation 2988/95 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

– created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).

Applicants will also be rejected if it turns out that[18]:

– during the award procedure they misrepresented information required as a condition for participating or failed to supply that information

– they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

Moreover, for the topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC and DIGITAL- ECCC-2024-

---

[16] See Articles 136 and 141 of EU Financial Regulation 2018/1046.

[17] Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision- making processes or obtain confidential information from public authorities to gain advantage.

[18] See Article 141 EU Financial Regulation 2018/1046.

DEPLOY-CYBER-07-SOCPLAT grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each topic) against the operational capacity and award criteria *(see sections 7 and 9)* and then ranked according to their scores.

For proposals with the same score (within a topic or budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:

1) Proposals focusing on a theme that is not otherwise covered by higher ranked proposals will be considered to have the highest priority.

2) The ex aequo proposals within the same topic will be prioritised according to the scores they have been awarded for the award criterion 'Relevance'. When these scores are equal, priority will be based on their scores for the criterion 'Impact'.

   When these scores are equal, priority will be based on their scores for the criterion 'Implementation'.

3) If this does not allow to determine the priority, a further prioritisation can be done by considering the overall proposal portfolio and the creation of positive synergies between proposals, or other factors related to the objectives of the call. These factors will be documented in the panel report.

4) After that, the remainder of the available call budget will be used to fund projects across the different topics in order to ensure a balanced spread of the geographical and thematic coverage and while respecting to the maximum possible extent the order of merit based on the evaluation of the award criteria.

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

⚠️ No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc*.

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access *(see also Funding & Tenders Portal Terms and Conditions)*. Please also be aware that for complaints submitted electronically, there may be

character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

1. Relevance

- Alignment with the objectives and activities as described in section 2

- Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level

- Extent to which the project would reinforce and secure the digital technology supply chain in the EU

- Extent to which the project can overcome financial obstacles such as the lack of market finance*

2. Implementation

- Maturity of the project

- Soundness of the implementation plan and efficient use of resources

- Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

3. Impact

- Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements

- Extent to which the project will strengthen competitiveness and bring important benefits for society

- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*.

May not be applicable to all topics (see specific topic conditions in section 2).

Award criteria	Minimum pass score	Maximum score
Relevance	3	5
Implementation	3	5
Impact	3	5
Overall (pass) scores	**10**	**15**

Maximum points: 15 points.

Individual thresholds per criterion: 3/5, 3/5 and 3/5 points. Overall threshold: 10 points.

Proposals that pass the individual thresholds AND the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on Portal Reference Documents.

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement (Data Sheet, point 1). Normally the starting date will be after grant signature. A retroactive starting date can be granted exceptionally for duly justified reasons but never earlier than the proposal submission date.

Project duration:

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs the indicative duration of the action is indicatively 36 months, other durations are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms the indicative duration of the action is indicatively 36 months, other durations are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS - Strengthening the SOC Ecosystem the indicative duration of the action is indicatively 36 months, other durations are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies the indicative duration of the action is indicatively 36 months, other durations are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER – Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations the indicative duration of the action is indicatively 36 months, other durations are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 -

- Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024) **-** the indicative duration of the action is indicatively 36 months, other durations are not excluded.

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverables will be mandatory for all projects:

- additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project.

Form of grant, funding rate and maximum grant amount

The grant parameters *(maximum grant amount, funding rate, total eligible costs, etc.)* will be

fixed in the Grant Agreement *(Data Sheet, point 3 and art 5)*. Project budget (maximum grant amount):

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC - National SOCs: indicatively between 1 and 2 million EUR per project but other amounts are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms: indicatively between 2 and 3 million EUR per project but other amounts are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS - Strengthening the SOC Ecosystem: one proposal for up to 2 million EUR.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies: indicatively between 3 and 5 million EUR per project but other amounts are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER – Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations: indicatively between 3 and 5 million EUR per project but other amounts are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024): indicatively between 2 and 4 million EUR per project but other amounts are not excluded.

The grant awarded may be lower than the amount requested. **The minimum budget for each topic as listed above is strongly recommended.**

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement *(see art 6 and Annex 2 and 2a)*.

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of action which applies to the topic *(see section 2)*.

Grants may NOT produce a profit (i.e. surplus of revenues + EU grant over costs). For- profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount *(see art 22.3)*.

Moreover, please be aware that the final grant amount may be reduced in case of non- compliance with the Grant Agreement *(e.g. improper implementation, breach of obligations, etc.)*

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement *(Data Sheet, point 3 and art 6)*.

Budget categories for this call:
- A. Personnel costs
    - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
    - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs

- C.1 Travel and subsistence

- C.2 Equipment

- C.3 Other goods, works and services

- D. Other cost categories

  - D.1 Financial support to third parties (for topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER)

  - D.2 Internally invoiced goods and services

- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:

  - average personnel costs (unit cost according to usual cost accounting practices)[19]: Yes

  - SME owner/natural person unit cost[20]: Yes

- travel and subsistence unit costs[21]: No (only actual costs)

- equipment costs:

  - depreciation (for topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS and DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02)

  - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC, DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT, DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH, DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER)

- other cost categories:

  - costs for financial support to third parties: compulsory for grants:

    - for topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER: maximum amount per third party EUR 60 000, unless a higher amount is required because the objective of the action would otherwise be impossible or overly difficult to achieve and this is duly justified in the Application Form.

      - In this instance, recipients of financial support to third parties have to co-finance the activity by minimum 50% of the total costs of the activity.
      - A minimum of 50% of the grant has to be reserved for financial support to third parties. The Commission estimates that 70% of the grant for financial support to third parties would allow the topic to be addressed appropriately.

- internally invoiced goods and services (unit cost according to usual cost accounting practices)[22]: Yes

---

[19] Decision of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

[20] Commission Decision of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7115).

[21] Commission Decision of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

[22] Decision of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).

- VAT: non-deductible VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)

- other:

    - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost

    - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed

    - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible

    - restrictions due to security:

        - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries

        - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible

    - other ineligible costs: No.

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement *(Data Sheet, point 4 and art 21 and 22)*.

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **80%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/10 days before starting date/financial guarantee (if required) – whichever is the latest.

There will be one or more **interim payments** (with cost reporting through the use of resources report) except for the topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07- LARGEOPER. In topic DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER, there might be **additional prefinancing payments** linked to a prefinancing report, in this case the first pre-financing will be reduced to the initial needs of the project.

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.

⚠️ Please be aware that payments will be automatically lowered if one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement *(see art 22)*.

Please also note that you are responsible for keeping records on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement *(Data Sheet, point 4)*. The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are normally requested from the coordinator, for the consortium. They must be provided during grant preparation, in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement *(art 23)*.

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement *(Data Sheet, point 4 and art 24)*.

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement *(Data Sheet point 4.4 and art 22)*.

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up* to their maximum grant amount

- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*

or

- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary)

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes

- protection of results: Yes

- exploitation of results: Yes

- rights of use on results: Yes

- access to results for policy purposes: Yes

- access to results in case of a public emergency: Yes

- access rights to ensure continuity and interoperability obligations: No

- special IPR obligations linked to restrictions due to security:

  - exploitation in eligible countries: Yes

  - limitations to transfers and licensing: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- communication and dissemination plan: Yes

- dissemination of results: Yes

- additional dissemination obligations: Yes

- additional communication activities: Yes

- special logo: both EU and European Cybersecurity Competence Centre logo

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for PAC Grants for Procurement: No

- specific rules for Grants for Financial Support: Yes for DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- specific rules for blending operations: No

- special obligations linked to restrictions due to security:

  - implementation in case of restrictions due to security or EU strategic autonomy: Yes

Other specificities

n/a

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

For more information, *see AGA — Annotated Grant Agreement*.

11. How to submit an application

All grant proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) create a user account and register your organisation

To use the Submission System (the only way to apply), all participants need to create an EU Login user account.

Once you have an EU Login account, you can register your organisation in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) submit the proposal

Access the Electronic Submission System via the Topic page in the Search Funding & Tenders section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 3 parts, as follows:

– Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online

– Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and upload it as a PDF file

– Annexes (*see section 5*). Upload them as PDF file (single or multiple depending on the slots). Excel upload is sometimes possible, depending on the file type.

The proposal must keep to the **page limits** (*see section 5*); excess pages will be disregarded.

For the topics DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC and DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT an expression of interest shall also be submitted no later than the 27 March 2025 at 17:00 Brussels time.

Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en. Applications must be submitted in the correct form, duly completed and dated. They must be submitted in electronic copy on https://cybersecurity- centre.europa.eu/funding-opportunities_en and signed by the person authorised to enter into legally binding commitments on behalf of the applicant organisation. The electronic version must contain the pdf versions of the application and other files as described in the call for expression of interest.

Documents must be uploaded to the **right category** in the Submission System otherwise the proposal might be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the IT Helpdesk webform (for the call for proposals) or via email to the address CNECT-ECCC-DEP@ec.europa.eu (for the call for expression of interest), explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the Online Manual. The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- Online Manual

- FAQs on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)

- Portal FAQ (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the IT Helpdesk.

Non-IT related questions should be sent to the following email address: CNECT-ECCC-DEP@ec.europa.eu

Please indicate clearly the reference of the call and topic to which your question relates (see cover page).

13. Important

> ⚠️ **IMPORTANT**
>
> - **Don't wait until the end —** Complete your application sufficiently in advance of the deadline to avoid any last-minute **technical problems**. Problems due to last minute submissions *(e.g. congestion, etc.)* will be entirely at your risk. Call deadlines can NOT be extended.
>
> - **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
>
> - **Funding & Tenders Portal Electronic Exchange System —** By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the Portal Terms & Conditions.
>
> - **Registration —** Before submitting the application, all beneficiaries, affiliated entities and associated partners must be registered in the Participant Register. The participant identification code (PIC) (one per participant) is mandatory for the Application Form.
>
> - **Consortium roles —** When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.
>
>   The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs must be justified in the application.
>
> - **Coordinator —** In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
>
> - **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any).
>
> - **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
>
> - **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.
>
> - **Balanced project budget —** Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully *(e.g. own contributions, income generated by the action, financial contributions from third parties, etc.)* You may be requested to lower your estimated costs, if they are ineligible (including excessive).

- **Completed/ongoing projects** — Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).

- **No-profit rule** — Grants may NOT give a profit (i.e. surplus of revenues + EU grant over costs). This will be checked by us at the end of the project.

- **No cumulation of funding/no double funding** — It is strictly prohibited to cumulate funding from the EU budget (except under 'EU Synergies actions'). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances be declared under two EU grants. If you would like to nonetheless benefit from different EU funding opportunities, projects must be designed as different actions, clearly delineated and separated for each grant (without overlaps).

- **Combination with EU operating grants** — Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice *(see AGA — Annotated Grant Agreement, art 6.2.E)*.

- **Multiple proposals —** Applicants may submit more than one proposal for *different* projects under the same call (and be awarded funding for them). Organisations may participate in several proposals.

  BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw the others (or they will be rejected).

- **Resubmission —** Proposals may be changed and re-submitted until the deadline for submission.

- **Rejection —** By submitting the application, all applicants accept the call conditions set out in this this Call Document (and the documents it refers to). Proposals that do not comply with all the call conditions will be **rejected**. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, they must be replaced or the entire proposal will be rejected.

- **Cancellation —** There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.

- **Language —** You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, *see section 12*).

- **Transparency —** In accordance with Article 38 of the EU Financial Regulation, information about EU grants awarded is published each year on the Europa website.

  This includes:
    – beneficiary names
    – beneficiary addresses
    – the purpose for which the grant was awarded
    – the maximum amount awarded.

  The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection —** The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the [Funding & Tenders Portal Privacy Statement](#).

<div align="right">**Annex 1**</div>

<div align="center">

Digital Europe types of action

</div>

The Digital Europe Programme uses the following actions to implement grants:

Simple Grants

Description: Simple Grants (SIMPLE) are a flexible type of action used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

SME Support Actions

Description: SME Support Actions (SME) are a type of action primarily consisting of activities directly aiming to support SMEs involved in building up and the deployment of the digital capacities. This type of action can also be used if SMEs need to be in the consortium and make investments to access the digital capacities.

Funding rate: 50% except for SMEs where a rate of 75% applies

Payment model: Prefinancing – (x) interim payment(s) – final payment

Coordination and Support Actions (CSAs)

Description: Coordination and Support Actions (CSAs) are a small type of action (a typical amount of 1-2 Mio) with the primary goal to support EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure and may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Grants for Procurement

Description: Grants for Procurement (GP) are a special type of action where the main goal of the action (and thus the majority of the costs) consist of buying goods or services and/or subcontracting tasks. Contrary to the PAC Grants for Procurement *(see below)* there are no specific procurement rules (i.e. usual rules for purchase apply), nor is there a limit to 'contracting authorities/entities'. Personnel costs should be limited in this type of action; they are in general used to manage the grant, coordination between the beneficiaries, preparation of the procurements.

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash- flow to finance the procurements) – payment of the balance

PAC Grants for Procurement

Description: PAC Grants for Procurement (PACGP) are a specific type of action for procurement in grant agreements by 'contracting authorities/entities' as defined in the EU Public Procurement Directives (Directives 2014/24/EU , 2014/25/EU and 2009/81/EC) aiming at innovative digital goods and services (i.e. novel technologies on the way to commercialisation but not yet broadly available).

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash- flow to finance the procurements) – payment of the balance

Grants for Financial Support

Description: Grants for Financial Support (GfS) have a particular focus on cascading grants. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations.

Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria.

In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third party costs.

Funding rate: 100% for the consortium, co-financing of 50% by the supported third party

Payment model: Prefinancing - second prefinancing (to provide the necessary cash- flow to finance sub-grants) – payment of the balance

Lump Sum Grants

Description: Lump Sum Grants (LS) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature). on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented only part of the lump sum will be paid.

Funding rate: 100%/50%/50% and 75% (for SMEs)

Payment model: Prefinancing – (x) interim payment(s)– final payment

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They

are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Annex 2

Eligibility restrictions under Articles 12(5) and (6) and 18(4) of the Digital Europe Regulation

Security restrictions Article 12(5) and (6)

If indicated in the Digital Europe Work Programme, and if justified for security reasons, topics can exclude the participation of legal entities *established* in a third country or DEP associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including DEP associated countries)[23].

This restriction is applicable for SO1 (High Performance Computing), SO2 (Artificial Intelligence) and SO3 (Cybersecurity), but at different levels.

- − In the case of SO3, the provision is implemented in the strictest way. When activated, only entities established in the EU AND controlled from the EU will be able to participate; entities from associated countries (which are normally eligible) can NOT participate — unless otherwise provided in the Work Programme.

- − In SO1 and SO2, entities established in associated countries and entities controlled from non-EU countries may participate, if they comply with the conditions set out in the Work Programme (usually:

    - − for the associated countries: be formally associated to Digital Europe Programme and receive a positive assessment by the Commission on the replies to their associated country security questionnaire.

    - − for the participants: submission of a guarantee demonstrating that they have taken measures to ensure that their participation does not contravene security or EU strategic autonomy interests).

⚠ EEA countries (and participants from EEA countries) benefit from a status equivalent to the Member States.

In order to determine the ownership and control status, participants[24] will be required to fill in and submit an ownership control declaration*as part of the proposal (and later on be requested to submit supporting documents) *(see Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls)*.

In addition, where a guarantee is required, the participants will also have to fill in the guarantee template*, approved by the competent authorities of their country of establishment, and submit it to the granting authority which will assess its validity.

The activation of these restrictions will also make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

Thus:
- − participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is also limited to entities

---

23 See Article 12(5) and (6) of the Digital Europe Regulation 2021/694.

24 Beneficiaries and affiliated entities, associated partners and subcontractors — except for entities that are validated as public bodies by the Central Validation Service.

- established in and controlled from eligible countries

    – project activities (included subcontracted work) must take place in eligible countries

    – the Grant Agreement provides for specific IPR restrictions.

Strategic autonomy restrictions Article 18(4)

If indicated in the Digital Europe Work Programme, calls can limit the participation to entities *established* in the EU, and/or entities established in third countries associated to the programme for EU strategic autonomy reasons[25].

The activation of these restrictions will make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

For more information, *see Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls*.

---

25   See Article 18(4) of the Digital Europe Regulation 2021/694.