Digital Europe Programme (DIGITAL)

Call for proposals

Cybersecurity and Trust
(DIGITAL-ECCC-2022-CYBER-03)

Version 1.0
15 September 2022

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	15.09.2022	▪ Initial version (new MFF).	
		▪	
		▪	
		▪	

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 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 2021-2022 Work Programme[2] by the **European Commission, Directorate-General for Communication, Networks, Content and Technology (DG CONNECT), on behalf of the European Cybersecurity Competence Centre (ECCC)**. Following a transfer of selected grant applications, ECCC will be responsible for the management of these grants.

Topic DIGITAL-ECCC-2022-CYBER-03-SOC is an EU Synergy call. Grants can be linked with another grant funded from any other EU funding programme. The grants under both calls will be managed as linked actions.

The call covers the following **topics**:

- **DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE - EU CybersecurityResilience, Coordination and Cybersecurity Ranges**

[1] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe programme for the period 2021-2027 (OJ L166, 11.05.2021).

[2] Commission Implementing Decision C/2021/7913 of 10.11.2021 concerning the adoption of the work programme for 2021-2022 and the financing decision for the implementation of the Digital Europe Programme.

- **DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs)**
- **DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE - Securing 5G Strategic Digital Infrastructures and Technologies**
- **DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS - Uptake of Innovative Cybersecurity Solutions**
- **DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION - Deploying the Network of National Coordination Centres with Member States**
- **DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE - Supporting the NIS Directive Implementation and National Cybersecurity Strategies**
- **DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES - Testing and Certification Capabilities**

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)
  - 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

Cybersecurity is at the heart of the digital transformation of the European Union. The Digital Europe Programme will strengthen the capabilities of the Union to protect its citizens and organisations aiming –amongst others- to improve the security of digital products and services. The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres, as soon as the Regulations establishing them will enter into force, will take care of the implementation of relevant actions.

The other supported Cybersecurity activities are specified in a dedicated Work Programme which will be later implemented by the ECCC as soon as operational, as specified in the ECCC legislation and in article 6(2) of the Digital Europe Regulation. In accordance with the Annex 1 of the Digital Europe Regulation, for first two years of implementation, the activities will focus on following three main work strands:

- support the deployment of cybersecurity infrastructure;
- strengthen cybersecurity uptake, specifically in sectors affected by the Covid-19 pandemic and the ensuing economic crisis.
- support the implementation of relevant EU legislation and political initiatives: in particular the cybersecurity strategy, NIS Directive, the Cybersecurity Act, the Regulation on the European Cybersecurity Competence Centre (ECCC) and the Network of National Coordination Centres, the cybersecurity Blueprint and Joint Cybersecurity Unit, the 5G security toolbox.

The participation is open to all eligible entities as established by Article 18 of the Digital Europe programme, in particular public sector as well as private sector organisations including SMEs and international organisations.

All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation. In that context, specific conditions apply to - DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS (see section 6).

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-2022-CYBER-03-CYBER-RESILIENCE - EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

Objectives

Proposals should address at least one of the following objectives:

- To strengthen the capacity of cybersecurity actors in the Union to monitor cyber-attacks and threats and supply chain risks, to react jointly against large incidents, and to improve relevant knowledge, skills and training. This objective will be pursued through the implementation of the Blueprint considering the important role of the Computer Security Incident Response Teams (CSIRTs) network and of the Cyber Crisis Liaison Organization Network (CyCLONe).

- To create, interconnect and strengthen cybersecurity ranges at European, national and regional level as well as within and across critical infrastructures, including in but not limited to sectors covered by the NIS Directive[3], in view to share knowledge and cybersecurity threat intelligence between stakeholders in the Member States, better monitor cybersecurity threats, and respond jointly to cyber-attacks.

Scope

Proposals addressing the first objective should build capacity of cybersecurity actors to react in a coordinated way to large scale cybersecurity incidents, while fostering the role of CSIRTs, the CyCLONe network and considering the Blueprint.

Such proposals should for example aim to provide stakeholders with structured test methodologies, vulnerability databases and forensic tools, or automated content delivery.

Proposals addressing the second objective should support the creation, operation, capacity increase and/or uptake of cybersecurity ranges, as well as foster networking between them in view to develop cybersecurity skills and expertise in key technologies (e.g. 5G, Internet of Things, Cloud, Artificial Intelligence, industrial control systems) as well as application sectors (e.g. health, energy, finance, transport, telecommunication, agri-food production, resource management) including consideration to cascading effects across sectors.

Such proposals should achieve at least one of the following:

- Exchange knowledge between cybersecurity ranges and create common data repositories.
- Support large-scale and cross-sector scenarios covering a wide range of adversaries and attack strategies, including for example cross centre serious gaming exercises; allow realistic traffic simulation that reflect network conditions.
- Support structured training and cybersecurity exercises to prepare cybersecurity defenders at both public and private organisations to enhance the protection and resilience of critical infrastructures, enterprises and communications networks; enable the conduct of hybrid trainings engaging all levels relevant to detecting, mitigating and preventing cyber-attacks (tactical, operational, strategic) while creating an environment where they can train communication, coordination and decision making.

Outcomes and deliverables

[3] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823).

The expected outcomes will be a strong capacity in the Member States to react in a coordinated way to large scale cybersecurity incidents, as well as top-level cybersecurity ranges offering advanced skills, knowledge and testing platforms.

KPIs to measure outcomes and deliverables

- Regarding the first objective:
  - Maturity analysis pre and post implementation to measure the change in cybersecurity capacity of the beneficiary(ies).
  - Report on interactions between the beneficiary(ies) and other stakeholders like peers or CSIRTs.
- Regarding the second objective:
  - Number of cyberranges created.
  - Number of cyberranges interconnected.
  - Maturity analysis pre and post implementation to measure the change in capacity of the cyberranges of the beneficiary(ies).
  - Number of sectors covered by specific cyberranges.
  - Number of common data repositories created.
  - Number of large-scale and cross-sector scenarios developed.
  - Number of supported structured training and cybersecurity exercises for public or private organisations to.

Targeted stakeholders

The first objective is open to all EU organisations with needs in cybersecurity.

For the second objective, the main targeted stakeholders are EU creators and providers of Cybersecurity Range services.

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)*
- For this topic, financial support to third parties is allowed *(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-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs)

Objectives

The objective will be to create, support and/or strengthen and interconnect cyber threat detection capacities, allowing for reinforced capacities to monitor and detect cyber threats, the creation of collective knowledge and sharing of best practices. In addition, data and capacities related to cybersecurity threat intelligence will be brought together from multiple sources (such as CSIRTs and other relevant cybersecurity actors) through cross-border platforms across the EU. The use of state-of-the-art AI, machine learning capabilities and common infrastructures will make it possible to more efficiently and more rapidly share and correlate the signals detected, and to create high-quality threat intelligence for national authorities and other stakeholders, thus enabling a fuller situational awareness and a more rapid reaction.

Scope

The aim is to improve cybersecurity resilience with faster detection and response to cybersecurity incidents and threats at national and EU level through the establishment of cyber threat detection and analysis capabilities, leveraging disruptive technologies, and sharing of information leading to increased situational awareness and stronger EU supply chains. Specifically, they should focus on at least one of the following

- Supporting entities dealing with cyber threat detection and analysis serving private (SMEs in particular) and/or public organisations with real-time monitoring and analysis of data from public internet network traffic to detect malicious activities and incidents that affect the resilience of network and information systems.
- Strengthening such entities by leveraging state of the art Artificial Intelligence (including Machine Learning techniques) and computing power to improve the detection of malicious activities, and dynamically learning about the changing threat landscape.
- Supporting information sharing among entities dealing with cyber threat detection and analysis or public authorities (including competent authorities and CSIRTs under the NIS Directive) or other public or private actors handling relevant threat information, facilitated through appropriate sharing agreements, while complying with all obligations related to privacy and personal data protection.

- Developing and deploying appropriate tools, platforms and infrastructures to securely share and analyse large data sets among entities dealing with cyber detection and threat analysis. Where possible and appropriate, existing building blocks will be re-used, including the results of relevant Connecting Europe Facility and Horizon 2020 projects.
- Supporting the increased availability, quality, usability and interoperability of threat intelligence data among relevant entities.

Additionally, proposals may focus on:

- Identify potential critical dependencies on foreign suppliers and solutions for threat intelligence and develop an EU supply chain on threat intelligence.
- Provide Member States bodies with threat intelligence and situational awareness capabilities helping to anticipate and respond to cyber-attacks, notably in the framework of the Blueprint/CyCLONe and the Joint Cybersecurity Unit;
- Bridge cooperation between various cybersecurity communities, e.g. civilian cybersecurity resilience, law enforcement, defence, taking into account cooperation frameworks such as the Blueprint/CyCLONe.

While these actions will enable capacity building, e.g. though the establishment or reinforcing of entities dealing with cyber detection and threat analysis serving private or public organisations, leveraging state of the art technology such as artificial intelligence and dynamic learning of the threat landscape, this will be combined with a call for expression of interest will be launched to select entities in Member States that provide the necessary facilities to host and operate cross-border platforms for pooling data on cybersecurity threat between several Member States (data potentially coming from various sources). A joint procurement will be launched to develop and operate capacities for the selected cross-border platforms.

Outcomes and deliverables

- World-class cyber threat detection capacities across the Union, strengthened with state of the art technology in areas such as AI.
- Sharing of Threat Intelligence between entities dealing with cyber detection and threat analysis.
- Threat intelligence and situational awareness capabilities supporting strengthened collaboration in the framework of the Blueprint/CyCLONe, as well as with law enforcement and defence.
- Actions may also contribute to cross-border platform for pooling data on cybersecurity threat between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools.

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 funded entities.
- Intensity of exchange of information between funded entities.
- Cyberthreat intelligence and situational awareness services developed

Targeted stakeholders

The target stakeholders are public and private actors, as well as consortia of either kind or combining them, which can support cyber threat detection and CTI sharing.

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)]*
- For this topic, financial support to third parties is allowed *(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-2022-CYBER-03-SEC-5G-INFRASTRUCTURE - Securing 5G Strategic Digital Infrastructures and Technologies

Objectives

The objective will be to support relevant entities in Member States, such as regulators of electronic communications or security agencies, in the implementation of their national cybersecurity strategies and legislation, in line with European 5G cybersecurity policy. This aims to support knowledge and capacity building for relevant national authorities regarding e.g. exchange of best practices; staff trainings; deployment of innovative evaluation methods; support standardisation actions; procurement of specialised services (e.g. audit and technical assessments).

Scope

Proposal should address at least one of the following two bullets:

- Support to 5G cybersecurity, notably to contribute to the goals and measures of the Recommendation and "toolbox" on 5G cybersecurity[4], as well as follow-up initiatives in that context.
- Piloting and supporting capacity building of security and interoperability aspects of open, disaggregate and interoperable technology solutions, such as Open RAN solutions. These solutions can explore new cooperation models and integrate innovative approaches provided by European SMEs possibly in cooperation with other players, while aiming at supporting the 5G cybersecurity toolbox goals, including supplier diversity and EU technology capacities.

The projects shall take into account activities in National Coordination Centres created on the basis of the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres where relevant, as well as taking into account other stakeholders. Projects involving national authorities from several EU Member States will be prioritised.

Outcomes and deliverables

- Trusted and secure 5G services.
- Support the cooperation between national authorities and private providers of technology services or equipment, in particular innovative European SMEs in cooperation with network and technology providers (e.g. vendors, mobile network operators and other players) on piloting, testing and integration of security and interoperability aspects of 5G interoperable, open and disaggregate solutions.

KPIs to measure outcomes and deliverables

- Number of Member States which received funding, with a clear national legislative framework implementing the EU 5G Toolbox in place.
- Number of knowledge and capacity building activities e.g., exchange of best practices; staff trainings; deployment of innovative evaluation methods; support standardisation actions; procurement of specialised services (e.g., audit and technical assessments) related to 5G security.
- Number of knowledge and capacity building activities related to security and interoperability aspects of innovative solutions, such as open, disaggregate and interoperable solutions.
- Number of test-beds, pilot projects on 5G interoperable, open and disaggregate solutions, such as Open RAN.

[4] See https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123. The toolbox was accompanied by Commission communication (COM(2020)50), which endorsed the Toolbox and identified areas of EU competence and/or EU added-value, such as funding programmes and projects.

Targeted stakeholders

All stakeholders, in particular national authorities (such as regulators of electronic communications or security agencies).

National authorities may associate themselves with private providers of technology services or equipment, in particular European SMEs, possibly in cooperation with network and technology providers, to pilot and develop security and interoperability aspects of innovative solutions, such as open, disaggregate and interoperable solutions.

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)*
- For this topic, financial support to third parties is allowed *(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-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS - Uptake of Innovative Cybersecurity Solutions

Objectives

To support the market uptake and dissemination of innovative cybersecurity solutions (notably in SMEs, as well as results from publicly funded research in the EU), improve knowledge and auditing of cybersecurity preparedness.

Scope

The focus will be on improving cybersecurity capabilities across the EU, notably for SMEs and public organisations, through both supply and demand support measures.

This may include awareness raising measures (where relevant in line with activities promoted by ENISA), or marketplace platforms supporting interaction between suppliers and adopters of cybersecurity solutions and training.

Proposals must address at least one, and ideally more, of the following:

- Cybersecurity protection services.
- Auditing of cybersecurity resilience of equipment and services.
- Security testing tools including static-analysis code scanning tools.
- Cybersecurity investigation tools, tracing the origins of cybersecurity threats.
- Incident response tools that fit into general operational and management cybersecurity strategies.
- Support to Coordinated Vulnerability Disclosure, in line with national policies where relevant.
- Funding and support for projects that improve and/or audit open-source software with regard to cybersecurity.
- Support for hackathons, cybersecurity challenges and conferences, and for engaging with relevant stakeholders including software development communities.
- Support to awareness raising, prevention, education, training, and gender balance in cybersecurity.

Outcomes and deliverables

The funding will contribute to some of the following:

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.
- Improve the security of ICT solutions, including open-source (e.g. establishment of bug bounty programmes).

KPIs to measure outcomes and deliverables

- Maturity analysis pre and post implementation to measure the change in cybersecurity capacity of the beneficiary(ies).
- How many and how market-ready innovative cybersecurity solutions have been adopted. (Also distinguishing EU funded ones.)
- Number of open-source solutions benefited from this action.

Targeted stakeholders

This topic targets in particular SMEs, but other applicants are not excluded.

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).* legal entities established in associated countries and legal entities that are established in the Union but are controlled from third countries can participate in calls for proposals and calls for tenders provided they comply with conditions set in Annex 3 of the Work Programme.
- 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-2022-CYBER-03-NAT-COORDINATION - Deploying the Network of National Coordination Centres with Member States

Objectives

With the creation of the European Cybersecurity Industrial, Technology and Research Competence Centre (Regulation (EU) 2021/887), the National Coordination Centres – working together through a network – will contribute to achieving the objectives of this regulation and to foster the Cybersecurity Competence Community in each Member State, contributing to acquire the necessary capacity. National Coordination Centres (NCC) will support cybersecurity capacity building at national and, where relevant, regional and local levels. They shall aim at fostering cross-border cooperation and at the preparation of joint actions as defined in the European Cybersecurity Industrial, Technology and Research Competence Centre and Network regulation.

Scope

The National Coordination Centre should carry out the following tasks:

- acting as contact points at the national level for the Cybersecurity Competence Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre in achieving its objectives and missions, in particular in coordinating the Cybersecurity Competence Community through the coordination of its national members;

- providing expertise and actively contributing to the strategic tasks of the European Cybersecurity Industrial, Technology and Research Competence Centre, taking into account relevant national and regional challenges for cybersecurity in different sectors;
- promoting, encouraging and facilitating the participation of civil society, industry in particular start-ups and SMEs, academic and research communities and other actors at Member State level in cross-border projects and cybersecurity actions funded through all relevant Union programmes;
- providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the European Cybersecurity Industrial, Technology and Research Competence Centre, and in full compliance with the rules of sound financial management, especially on conflict of interests. This should be done in close coordination with relevant NCPs set up by Member States, such as those funded under the Horizon Europe topic: "HORIZON-CL3-2021-SSRI-01-03: National Contact Points (NCPs) in the field of security and cybersecurity";
- seeking to establish synergies with relevant activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of, and in particular in those policies stated in the national cybersecurity strategies;
- where relevant, implementing specific actions for which grants have been awarded by the European Cybersecurity Industrial, Technology and Research Competence Centre, including through provision of financial support to third parties in line with article 204 of Regulation (EU, Euratom) 2018/1046 under the conditions specified in the grant agreements concerned; such support should in particular aim at strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs);
- promoting and disseminating the relevant outcomes of the work of the Network, the Cybersecurity Competence Community and Competence Centre at national, regional or local level;
- assessing requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the National Coordination Centre;
- advocating and promoting involvement by relevant entities in the activities arising from the European Cybersecurity Industrial, Technology and Research Competence Centre, the Network of National Coordination Centres, and the Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments and deployments.

Proposals are expected to further specify the activities listed above and possibly other relevant activities. The funding can cover the capacity building and the functioning of the National Coordination Centres for up to 2 years.

Proposals are expected to demonstrate that they are able to coordinate respective activities with relevant European Digital Innovation Hubs created pursuant to article 16 of the Regulation establishing the Digital Europe Programme.

The Commission considers an EU contribution of up to about EUR 1 million appropriate for the capacity building and the functioning of the National Coordination Centres over 2 years. The Commission further considers that as part of the same proposal, applicants may request another EUR 1 million to be provided in the form of financial support to third parties, with the aim of supporting the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs).

This call targets exclusively National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

Outcomes and deliverables

Setup and operation of National Coordination Centres in Member States.

KPIs to measure outcomes and deliverables

- Entities being engaged as members of the national cybersecurity community.
- Actions to assist and reinforce the expertise of cybersecurity community members, as well as synergies between activities of these members and synergies with relevant cyber policy goals.
- Entities (including from civil society, SMEs, academia and research) being supported to participate in relevant, national and international/ EU, cybersecurity projects and collaboration activities.
- Actions to promote the participation mentioned in the previous point, including assistance to apply for funding opportunities, prizes and competitions, opportunities to exploit results, etc.
- Actions to promote the expertise and achievements of the members of the cybersecurity community.
- Collaboration actions with other NCCs and with the ECCC.

Targeted stakeholders

This call targets National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[5].

Type of action and funding rate

[5] Article 7(3) of Regulation EU (2021) 887 provides that NCCs may receive a grant from the Union without an open call for proposals in relation to carrying out their tasks, on the basis of a Commission assessment recognising the NCC as having the necessary capacity to manage funds to fulfil the mission and objectives laid down in that Regulation. The criteria and process for such assessment are specified in Commission Communication C(2021) 7412 on Guidelines on the assessment of the capacity o of National Coordination Centres to manage funds to fulfil the mission and objectives laid down in Regulation (EU) 2021/887.

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)*
- For this topic, financial support to third parties is allowed *(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-2022-CYBER-03-NIS-DIRECTIVE - Supporting the NIS Directive Implementation and National Cybersecurity Strategies

Objectives

The action focuses on Member States and European capacity building and the enhancement of cross-border cooperation on cybersecurity at technical, operational and strategic levels. Proposals should contribute to achieving these objectives:

- Development of trust and confidence between Member States.
- 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 Operators of Essential Services and for digital service providers in the EU.
- Improved security of network and information systems in the EU.
- More alignment and harmonisation of Member States' implementations of the NIS Directive[6].

Scope

[6] References to the NIS Directive in this section shall also include sectoral lex specialis rules to the NIS, and in particular the Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM/2020/595 final, and the authorities and procedures set up under those rules.

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

- User-centred implementation, validation, piloting and deployment of technologies, tools and IT-based solutions[7], processes and methods for monitoring, preventing, detecting and handling cybersecurity incidents (including in the context of cross-border cybersecurity threats and cross sector context) in EU Member States.
- Collaboration, communication, awareness-raising activities, knowledge exchange and training, including using cybersecurity ranges, of public and private organisations working on the implementation of the NIS Directive.
- 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.

Furthermore, Member States can define additional critical sectors, including public administrations, and identify operators for their countries.

In addition, the NIS Directive applies to providers of the following types of digital services (DSP):

- Online marketplace.
- Online search engine.
- Cloud computing service.

Outcomes and deliverables

Proposals are expected to deliver on at least two of the following results:

- Enable the Member States to limit the damage of cybersecurity incidents, including economic, social, environmental, or political damage, while reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Improve compliance with the NIS Directive, higher levels of situational awareness and crisis response in Member States.
- Contribute to enhanced cooperation, preparedness and cybersecurity resilience of the EU.

KPIs to measure outcomes and deliverables

- Number of actions performed to develop trust and confidence between Member States.
- Number of cooperative actions performed with/by CSIRTs (including in relation to the CSIRT Network) or Operators of Essential Services.

[7] Where possible, open-source software should be preferred.

- Number of twinning schemes and their actual use.
- Number of resilience building measures.
- Improvement in compliance with the NIS Directive by the beneficiary(ies).

Targeted stakeholders

The support targets relevant Member State competent authorities, which play a central role in the implementation of the NIS Directive, Computer Security Incident Response Teams (CSIRTs) including sectorial CSIRTs, Security Operation Centres (SOC), Operators of Essential Services (OES), digital service providers (DSP), industry stakeholders (including Information Sharing and Analysis Centres- ISACs), and any other actors within the scope of the NIS Directive[8].

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, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply *(see section 6)*
- 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-2022-CYBER-03-TEST-CERT-CAPABILTIES - Testing and Certification Capabilities

[8] The proposed topic should take into account revisions to the NIS Directive as relevant, including the list of sectors, sub-sector and entities in Annexes I and II of the legal proposal. The European Commission proposal significantly widens the scope of the NIS Directive, going beyond current OES and DSPs categories.

Objectives

The objective of this topic is to increase and facilitate security and interoperability testing capabilities and certification of connected ICT systems. This aims to improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 ("Cybersecurity Act").

Scope

Proposals should address at least one of the following:

- Support capacity building for national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies including for thread-based penetration testing; e.g. for the acquisition of certification testbeds; exchange of best practices and staff trainings; deploy innovative evaluation methods for specific ICT products or components; support standardisation actions (e.g. creation of protection profiles or adoption/improvement of standards used in certification schemes). This shall take into account activities in National Coordination Centres where relevant.
- Support SMEs to test and certify ICT products, ICT services or ICT process they sell. The priority will be given to proposals demonstrating a positive impact in sectors affected by the COVID-19 crisis (e.g., health sector).
- Provide support for SME users of ICT equipment to audit their infrastructures in term of cybersecurity resilience.
- Support standardisation actions (e.g., creation of protection profiles or adoption/improvement of standards used in certification schemes), considering activities by European and international standardisation organisations as appropriate.
- Support cyber-security and interoperability testing capabilities on 5G disaggregated and open solutions.

Where relevant, support will focus on certification schemes under the Cybersecurity Act, while it could also be available for technical areas not yet covered by schemes under the Cybersecurity Act.

Outcomes and deliverables

The funding is expected to:

- Strengthen national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies.
- Improve the cybersecurity and interoperability testing capabilities in all Member States, including in the area of 5G disaggregated and open solutions and trusted chips.
- Support SMEs to audit their infrastructure in view of improving their cybersecurity protection.
- Support actions in the area of standardisation.

KPIs to measure outcomes and deliverables

- Number of supported certification testbeds set up and innovative evaluation methods deployed for specific ICT products or components by national cybersecurity certification authorities, conformity assessment bodies;
- Additional certification and testing services provided by a beneficiary as a result of the activities
- Standardisation actions with European and international standardisation organisations that were supported, e.g. number or novelty of standards and specifications published in reference to evaluation tools and methods utilised by a beneficiary;
- Knowledge and capacity building activities e.g., exchange of best practices, staff trainings;
- Increase in the number or expansion of scope of ICT products, services or processes of SMEs that received support for their testing and certification;
- ICT equipment's audits in terms of cybersecurity resilience by SMEs which were supported.
- Cybersecurity and interoperability testing capabilities supported on 5G disaggregated and open solutions or on chips.

Targeted stakeholders

This topic targets in particular national cybersecurity certification authorities, conformity assessment bodies, accreditation bodies, universities and other relevant stakeholders. National Coordination Centres created on the basis of Regulation (EU) 2021/887, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, may respond to this open call with a view to allocating Financial Support to Third Parties.

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 allowed *(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 available call budget is **EUR 176.500.000**. This budget might be increased by maximum 20%.

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

Topic	Topic budget
DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE	EUR 15.000.000
DIGITAL-ECCC-2022-CYBER-03-SOC	EUR 72.500.000
DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE	EUR 10.000.000
DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS	EUR 32.000.000
DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION	EUR 22.000.000
DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE	EUR 20.000.000
DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES	EUR 5.000.000

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:	29 September 2022
Deadline for submission:	24 January 2023 – 17:00:00 CET (Brussels)
Evaluation:	March 2023

Information on evaluation results:	May 2023
GA signature:	October 2023

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** *(to be uploaded)*:
  - detailed budget table: not applicable
  - CVs of core project team: not applicable
  - activity reports of last year: not applicable
  - list of previous projects : not applicable
  - **ownership control declaration: applicable**
  - For the topic DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE: declaration confirming beneficiaries are considered OES/DSP by their MS.

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). 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

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)) for all topics
  - EEA countries (Norway, Iceland, Liechtenstein) for all topics
  - **For topic DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS only:** countries associated to the Digital Europe Programme (list of countries) or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature.[9] All applicants from an associated countries have to present a guarantee approved by the country, confirming they will comply with the conditions set out in the work programme Annex 3.

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[10] 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 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)*.

Specific cases

[9] Beneficiaries from countries with ongoing negotiations may participate in the call and can sign grants if the negotiations are concluded before grant signature (with retroactive effect, if provided in the agreement). Proposals including entities from countries which are in ongoing negotiations for an association agreement that does not enter into force before the signature of the grant might be declared ineligible. In those cases the consortium will be asked to replace the participant concerned (or redistribute the tasks between the other participants). If this is not possible and the consortium cannot propose any other acceptable solution, the proposal will have to be rejected.

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

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[11].

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'[12]. ⚠ 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).

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)[13] and entities covered by Commission Guidelines No 2013/C 205/05[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).

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

Consortium composition

Proposals must be submitted by:

for topics DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE:

- minimum 3 independent applicants (beneficiaries; not affiliated entities)

For all 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).

11 See Article 197(2)(c) EU Financial Regulation 2018/1046.
12 For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.
13 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.
14 Commission guidelines No 2013/C 205/05 on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

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 allowed in DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE, DIGITAL-ECCC-2022-CYBER-03-SOC, DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE, DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION and DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES for grants under the following conditions:

- 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.

Your project application must clearly specify why financial support to third parties is needed, how it will be managed and provide a list of the different types of activities for which a third party may receive financial support. The proposal must also clearly describe the results to be obtained.

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:

- 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 clearing (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 clearing may have to be provided before grant signature. The granting authority will assess the need for clearing 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 clearing.

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

[15] See Commission Decision 2015/544/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

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 refused 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).

8. Evaluation and award procedure

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.

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

An **evaluation committee** (composed or 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 are 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:

- **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*****
- **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
- **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. Retroactive application can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration:

For topic DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE the indicative duration of the action is 36 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-SOC the indicative duration of the action is 36 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE the indicative duration of the action is 12 to 36 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS the indicative duration of the action is up to 36 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION the indicative duration of the action is 24 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE the indicative duration of the action is 36 months, but other durations are not excluded

For topic DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES the indicative duration of the action is 36 months, but other durations are not excluded

Extensions are possible, if duly justified and through an amendment.

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-2022-CYBER-03-CYBER-RESILIENCE: between EUR 1 million and EUR 4 million per project

- for topic DIGITAL-ECCC-2022-CYBER-03-SOC: between EUR 1 million and EUR 10 million
- for topic DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE: between EUR 1 million and EUR 3 million per project
- for topic DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS: between EUR 1 million and EUR 5 million per project
- for topic DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION: between EUR 1 million and EUR 2 million per project
- for topic DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE: between EUR 1 million and EUR 5 million per project
- for topic DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES: between EUR 0,5 million and EUR 1 million per project

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 topics DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE, DIGITAL-ECCC-2022-CYBER-03-SOC, DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE, DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION and DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES)
  - 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): Yes
  - SME owner/natural person unit cost[19]: Yes
- travel and subsistence unit costs[20]: No (only actual costs)
- equipment costs:
  - depreciation (for topic DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION)
  - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE, DIGITAL-ECCC-2022-CYBER-03-SOC, DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE, DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS, DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE, DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES)
- other cost categories:
  - costs for financial support to third parties: allowed for grants:
    - for topics DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE, DIGITAL-ECCC-2022-CYBER-03-SOC, DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE, DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION: 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
    - for topic DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES: maximum amount per third party EUR 100 000, 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.

[19] 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)7715).

[20] 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).

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

- 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
  - EU Synergies call: Yes, costs can be charged to several EU Synergies grants, provided that the funding under the grants does not go above 100% of the costs and contributions declared to them (for topic DIGITAL-ECCC-2022-CYBER-03-SOC)
  - 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). There will be one or more **additional prefinancing payments** linked to a prefinancing report for topic DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES.

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 formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount *(by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc)*. It is however important that the requested amount is covered and that the guarantee(s) are sent to us 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.

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
  - first exploitation obligation in eligible countries: No
  - 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 communication activities: Yes
- special logo: both EU and 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: No
- 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 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 EULogin 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.

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, 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 please contact your National Coordination Centre. In cases where this is not practical, please submit questions using this form.

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).
- No-profit rule (n/a for FPAs) — 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 double funding (n/a for FPAs) — There is a strict prohibition of double 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 declared to two different EU actions.
- 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).
- Combination with EU operating grants (n/a for FPAs) — 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 Model 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 a 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 one of them (or it 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.

Annex 1

Digital Europe types of action

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: 50%

Payment model: Prefinancing – second (third) prefinancing (as there is no cost reporting) – 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)[21].

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 EU MS or EU legal entities will be able to participate — with no exceptions.

- In SO1 and SO2, entities controlled by third countries or third country legal entities may be able to participate if they comply with certain conditions set up in the Work Programme. To that end, additional rules will be imposed on those legal entities, which need to be followed if they want to participate.

The activation of this article will be 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.

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[22].

The application of this article 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*.

[21] See Article 12(5) and (6) of the Digital Europe Regulation 2021/694

[22] See Article 18(4) of the Digital Europe Regulation 2021/694.