EUROPEAN
COMMISSION

Brussels, 10.11.2021
C(2021) 7913 final

ANNEX

ANNEX

to the

Commission Implementing Decision

on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 - 2022

DIGITAL EUROPE
Cybersecurity

Work Programme 2021-2022

INTRODUCTION

Digital technologies are profoundly changing our daily life, our way of working and doing business, the way we understand and use our natural resources and environment and the way people interact, communicate and educate themselves. The von der Leyen's Commission has presented an ambitious strategy on shaping Europe's digital future on 19 February 2020[1]. The "Council conclusions of 9 June 2020[2] confirmed this ambition.

The COVID-19 crisis has further highlighted the critical role of digital technologies and infrastructures in our lives and demonstrated how our societies and economies rely on digital solutions. Moreover, it has accelerated the digital transition. The crisis has also confirmed how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world.

In December 2020, the Commission and the High Representative presented the EU's Cybersecurity Strategy for the Digital Decade[3], which inter alia sets out the objective to develop the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies. The Strategy also acknowledges that EU policies and investment in cybersecurity are a cornerstone of the EU Security Union Strategy.[4] The efforts needed to achieve the aforementioned goals are not limited to Research and Development. The EU must drastically improve its digital capacities. This includes the deployment of digital technologies, as well as the necessary digital skills for all EU workforce. Europe must also develop key digital infrastructures, innovate and strengthen its industrial base, enhance its resilience and flexibility both in terms of technologies and supply chains. Delivering this will require massive public and private investment and common efforts that no Member State alone could secure. In that context, the European data strategy has announced a High Impact project on European data spaces, encompassing data sharing architectures and governance mechanisms, as well as the European federation of energy-efficient and trustworthy cloud infrastructures and related services. The Digital Europe Programme will also contribute to the achievement of the digital targets, as outlined in the communication: "2030 Digital Compass: the European way for the Digital Decade[5]. Indeed, the Digital Europe Programme work strands will provide key support to the digital transformation of the economy in the next decade, as well as to achieve European digital sovereignty[6] by deploying key technological capabilities. The Digital Europe Programme will also contribute to the achieve the goals highlighted in the Commission proposal for a Regulation on a Single Market For Digital Services (the Digital Services Act - DSA)[7] and a Regulation on contestable and fair markets in the digital sector (the Digital Markets Act - DMA)[8] through actions

[1] https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[2] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

[3] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020)18)

[4] Communication to the European Parliament and the Council on the EU Security Union Strategy (COM/2020/605 final)

[5] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[6] By strengthening the EU's open strategic autonomy and resilience.

[7] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN

[8] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

aiming to create a safer digital space in which the fundamental rights of all users of digital services are protected and through actions that aim to establish a level playing field to foster innovation, growth, and competitiveness.

This document sets out the Cybersecurity Work Programme for part of the actions to be implemented in the first two years of the Digital Europe Programme under objective 3 : Cybersecurity and Trust. It follows extensive consultations with the Member States, stakeholders and the public on drafts of the strategic orientations. It uses as a reference point the Annex 1 of the Digital Europe Programme Regulation[9].

THE DIGITAL EUROPE PROGRAMME OBJECTIVES

The Digital Europe Programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, the deployment of these technologies, and their best use for critical sectors like energy and environment, manufacturing, agriculture and health.

The Digital Europe Programme is strategic in supporting the digital transformation of the EU industrial ecosystems. The funding will be available for EU Member States as well as other countries associated to the Digital Europe Programme (unless otherwise specified in the topic description, tender specifications and call for proposals).

The Digital Europe Programme also targets upskilling to provide a workforce for these advanced digital technologies. It supports industry, SMEs, and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs (EDIH). The Digital Europe Programme will accelerate the economic recovery and drive the digital transformation of Europe.

The twin transitions to a green and digital Europe remain the defining challenges of this generation. This is reflected throughout the Commission's proposals. The Digital Europe Programme will deliver on the goals set out in the European data strategy of realising the vision for a genuine single market for data. It will help bring European human centred AI-solutions as set out in the White Paper on AI[10] as well as promote the deployment of other key digital technologies with respect for Union values[11], and from a human-centric perspective. The Digital Europe Programme will unleash the powers of digital technologies to reach Europe's common climate and environmental goals as set out in the European Green Deal, including being climate neutral by 2050, as well as strengthen the resilience of Europe's industry and increase its open strategic autonomy.

With the actions contained in this Work Programme, Digital Europe will build up advanced cybersecurity equipment, tools and data infrastructures. It will support the development and best use of European knowledge and skills related to cybersecurity, promote the sharing of best practices and ensure a wide

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3APE_13_2021_INIT

[10] https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-european-approach-excellence-and-trust

[11] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407

deployment of the state–of-the-art cybersecurity solutions across the European economy to guarantee the resilience, integrity and trustworthiness of the Digital Single Market.

The Cybersecurity strategy identifies, as areas for EU action: resilience, technological sovereignty and leadership of the Union. It recognises that the EU's critical infrastructure and essential services are increasingly interdependent and digitised. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, the whole supply chains which make them available, as well as the underlying internet infrastructure need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.

THIRD COUNTRY PARTICIPATION

Dependencies and vulnerabilities in cybersecurity can open the door to increased foreign influence and control over key industrial assets as well as over providers of critical infrastructure and essential services. This in turn can lead to disadvantageous knowledge transfers, long-term economic costs, and make Europe susceptible to undue foreign influence. Cybersecurity incidents can be either accidental or the deliberate action of criminals, state and other non-state actors. Cybersecurity attacks on infrastructure, economic processes and democratic institutions, undermine international security and stability and the benefits that cyberspace brings for economic, social and political development.

Therefore, the security interests of the Union in the area of cybersecurity require building capacity to secure sensitive infrastructures through cybersecurity solutions and reducing dependence on other parts of the globe for the most crucial technologies. All actions under this Work Programme aim at increasing the EU's collective resilience against cybersecurity threats. Furthermore, several actions in this Work Programme will establish tools, infrastructures and resources intended specifically for the use of cybersecurity authorities in Member States in defending against criminal and/or politically motivated cyber threats, including especially supply-chain attacks. This means in order to protect essential security interests of the Union, the implementation of cybersecurity topics (calls for proposals and calls for tenders) under the Digital Europe Programme should depend on legal entities (e.g. providers) established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.

Because of their criticality, participation to all the calls funded under this Work Programme will be subject to the provisions of article 12(5) of the Digital Europe Programme Regulation. In addition, 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 under topics 1.1.4 (Uptake of Innovative Cybersecurity Solutions) and 1.2.2 (Cybersecurity community support), provided they comply with conditions set in Annex 3 of this Work Programme.

At the same time, the Digital Europe Programme is open for collaboration with third countries. Specific conditions for the association or partial association of third countries to the Programme are laid down in article 10 of the Digital Europe Programme Regulation.

The conditions for international cooperation with third countries, international organisations and bodies established in third countries are specified in article 11 of the Digital Europe Programme Regulation.

Cooperation and association agreements may be subject to adequate security, IP protection and reciprocity guarantees.

Participation to the actions is intended to be open to all eligible third countries according to the association agreement they have signed at the time of signature of the grant agreement, even though the text of the actions only refer to Member States.

INDICATIVE BUDGET AND IMPLEMENTATION

Digital Europe is implemented by means of multiannual Work Programmes. There are four independent Work Programmes. This Work Programme covers Specific Objective 3: Cybersecurity and Trust topics that will be implemented by the Commission on behalf of the European Cybersecurity Industrial, Technology and Research Competence Centre with the Network of National Coordination Centres (ECCC)[12] . The other three Work Programmes are devoted to the following intervention areas: 1) High Performance Computing (implemented under indirect management); 2) the network of European Digital Innovation Hubs; 3) Data, AI, Cloud, Quantum Communication Infrastructure, advanced digital Skills and deployment activities for the best use of these technologies. Synergies and complementarities of the activities in the various Work Programmes will be ensured.

Until the ECCC has the capacity to implement its own budget, the European Commission will implement the actions under this Work Programme in direct management on behalf of the ECCC.

The budget for the Cybersecurity actions covered by this Work Programme is EUR 269 million[13] distributed as follows:

- A budget of EUR 177 million for actions related to the "cyber-shield" announced in the EU Cybersecurity Strategy[14], including Security Operation Centres (SOC);
- A budget of EUR 83 million for actions supporting the Implementation of relevant cybersecurity EU Legislation;
- A budget of EUR 9 million for programme support actions, including evaluations and reviews.

In addition, actions supporting the deployment of the Secure Quantum Communication Infrastructures (QCI) are included in the Digital Europe Work Programme for 2021-2022, with an indicative budget of EUR 170 million.

Table 1: Breakdown of global expenditure per type of action.

[12] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research.

[13] The amounts drawn from the 2022 budget are subject to the availability of the appropriations provided for in the draft budget for 2022 after the adoption of the budget 2022 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

[14] JOIN(2020)18

Year	Budget line	Amounts to be implemented in direct management (in million EUR)		Total per budget line, per year (in million EUR)
		Calls for proposals - grants	Calls for tender - procurement	
2021	**Specific Objective 3 (02 04 01 11 02)**	43	3	46
2022	**Specific Objective 3 (02 04 01 11 02)**	184	39	223
Grand total				269

The budget figures given in this Work Programme are indicative and subject to change.

MULTI COUNTRY PROJECTS: CO-INVESTMENTS FROM PUBLIC AND PRIVATE SECTOR AND LINKS WITH OTHER PROGRAMMES

Most actions foreseen in the Programme require co-investments from the public and private sector. The modes of these co-investments are described in the relevant parts of the various Digital Europe Work Programmes. Several actions relate to cross-border or multi-country projects (MCP) as foreseen in the EU Recovery and Resilience Facility (RRF). In addition to the RRF, several programmes at EU, national and regional level will also contribute to these projects. The table below summarises the expected contributions.

Table 2: Multi Country Projects relevant for this Work Programme

MCP relevant for this Work Programme	Actions in Digital Europe	Other contributing programmes
Security Operation Centres (SOC)	The creation, interconnection and strengthening of Security Operations Centres (SOC) can improve cybersecurity resilience with faster detection and response to cybersecurity incidents at national and EU level by leveraging disruptive technologies and sharing of information leading to increased situational awareness and stronger EU supply chains. A key element will be capacity building, e.g. by leveraging artificial intelligence and dynamic learning of the threat landscape.	RRF

CALLS STRUCTURE AND PLANNING

Calls for Proposals

The global budgetary envelope reserved for grants under this Work Programme is 227 million EUR to be committed in 2022.

Table 3: List of topics in the first call for proposals (grants) under this Work Programme

Area	Topics in the Work Programme	Budget (in million EUR)
European "cyber-shield"	Support to cybersecurity in the health sector	10
Support to implementation of relevant EU legislation	Deploying the Network of National Coordination Centres with Member State	33
Total		**43**

Table 4: List of topics in the second call for proposals (grants) under this Work Programme

Area	Topics in the Work Programme	Budget (in million EUR)
European "cyber-shield"	EU cybersecurity resilience, coordination and cybersecurity ranges	15
	Capacity building of Security Operation Centres	80
	Securing 5G strategic digital infrastructures and technologies	10
	Uptake of innovative cybersecurity solutions	32
Support to implementation of relevant EU legislation	Deploying the Network of National Coordination Centres with Member State	22
	Supporting the NIS Directive implementation and national cybersecurity strategies	20
	Testing and certification capabilities	5
Total		**184**

Calls for tender

In addition to the calls for proposal, a set of actions will be implemented by procurement either using Framework contracts or open calls for tenders.

The global budgetary envelope reserved for procurement under this Work Programme 42 million EUR out of which 3 million EUR to be committed in 2021 and 39 million EUR in 2022.

Contents

1 Actions for Cybersecurity and Trust

Cybersecurity is at the heart of the digital transformation of the European Union. In line with the Cyber security strategy published in December 2020, the European Union must create a strong "cyber-shield" to protect its citizens, industries, and values. To do so, the Union will invest in a top of the range, comprehensive network of Security Operation Centres (SOC), while strengthening its cyber security industry and skills to guarantee its autonomy.

The Digital Europe Programme will strengthen the capabilities of the Union for resilience and protection of its citizens and organisations aiming –amongst others- to improve the security of digital products and services. In the first two years of implementation, the activities will aim to:

- 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, The Directive on security of network and information systems (the NIS Directive), the Cybersecurity Act, the Regulation on the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres, the cybersecurity Blueprint and Joint Cyber Unit, and the 5G cybersecurity toolbox;
- Raise awareness and foster cybersecurity skills and training.

All activities should give due consideration to fundamental values, notably relating to privacy and data protection.
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 NGOs.

1.1 European "Cyber-Shield"

The EU Cybersecurity Strategy[15] announced an EU "cyber-shield" bringing together in particular EU policies and investment for better operational cooperation and situational awareness, such as SOCs, Information Sharing and Analysis Centres (ISACs), and the Joint Cyber Unit (JCU).

1.1.1 EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

Objective

The implementation of this topic has two main 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

[15] See https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 and JOIN(2020)18

Blueprint and the future Joint Cyber Unit 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[16], 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, the future Joint Cybersecurity Unit, and taking into account the Blueprint.

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. This action will aim to:

- 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;
- provide additional services to stakeholders such as structured test methodologies, vulnerability database and forensic tools; develop of automated content delivery options supporting specific job profiles.

Outcomes and deliverables

[16] 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.

Type of action	SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries)
Indicative Budget	EUR 15 million
Indicative time of call opening	Second call
Indicative duration of the action	36 months
Indicative budget per grant (EU contribution)	EUR 2 - 4 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.1.2 Capacity Building Of Security Operation Centres (SOC)

Objective

The objective will be to create, support and/or strengthen and interconnect SOCs at regional, national and EU level. This will allow 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 SOCs, leveraging disruptive technologies, and sharing of information leading to increased situational awareness and stronger EU supply chains. Specifically:

- Supporting existing SOCs or establishing national, regional or sectoral SOCs 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 SOCs 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 public authorities (including competent authorities and CSIRTs under the NIS Directive), as well as with other SOCs (e.g. operated by private entities), 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 SOCs. 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 SOCs and relevant entities;
- Identify potential critical dependencies on foreign suppliers and solutions in the area of 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 and the Joint Cybersecurity Unit.

To achieve this aim, the following activities are foreseen:

- Grants will be made available to enable capacity building, e.g. though the establishment or reinforcing of SOCs serving private or public organisations, leveraging state of the art technology such as artificial intelligence and dynamic learning of the threat landscape
- A call for expression of interest will be launched to select entities in Member Statesthat 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). The call for expression of interest will also build up the planning and design of necessary tools and infrastructures.
- Building on the call for expression of interest, a joint procurement will be launched to develop and operate capacities for the selected cross-border platforms, including advanced tools and infrastructures to securely share and analyse large data sets and threat intelligence among the selected cross-border platforms (e.g. highly-secure infrastructure or advanced data analytics aimed at significantly improving the ability to analyse large sets of data)

Outcomes and deliverables

- Several cross-border platform(s) for pooling data on cybersecurity threat between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools;
- World-class SOCs across the Union, strengthened with state of the art technology in areas such as AI;
- Sharing of Threat Intelligence between SOCs, and information sharing agreements with competent authorities and CSIRTs;
- Threat intelligence and situational awareness capabilities supporting strengthened collaboration in the framework of the Blueprint/CyCLONe and the Joint Cybersecurity Unit, as well as with law enforcement and defence.

Capacity building activity:

Type of action	Simple grant (50% co-funding rate)
Indicative Budget	EUR 80 million
Indicative time of call opening	Second call
Indicative duration of the action	36 months
Indicative budget per grant (EU contribution)	EUR 7 – 10 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

Deployment and running of advanced tools and infrastructures:

Type of action	Joint procurement
Indicative Budget	EUR 30 million
Indicative year of procurement	2022
Indicative duration of the action	36 months
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.1.3 Securing 5G Strategic Digital Infrastructures And Technologies

Objective

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

- Support to 5G cybersecurity, notably to contribute to the goals and measures of the Recommendation and "toolbox" on 5G cybersecurity[17], 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 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.

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,

[17] 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.

testing and integration of security and interoperability aspects of 5G interoperable, open and disaggregate solutions.

Type of action	Simple grant (50% co-funding rate)
Indicative Budget	EUR 10 million
Indicative time of call opening	Second call
Indicative duration of the action	12 – 36 months
Indicative budget per grant (EU contribution)	EUR 1 to 3 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.1.4 Uptake Of Innovative Cybersecurity Solutions

Objective

To support the market uptake and dissemination of innovative cybersecurity solutions (notably from 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.

The types of tools covered must include at least one 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:

- 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 open-source solutions (e.g. establishment of bug bounty programmes).

Type of action	SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries)
Indicative Budget	EUR 32 million
Indicative time of call opening	Second call
Indicative duration of the action	Up to 36 months
Indicative budget per grant (EU contribution)	EUR 2 to 5 million
Implementation	European Commission on behalf of the ECCC
Security	On the basis of article 12(5) of the Digital Europe Programme Regulation, 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 this document

1.1.5 Support To Cybersecurity In The Health Sector

Objective

The action will support cybersecurity resilience in healthcare and public health institutions, which have been put under particular stress over the recent years, especially further to the COVID-19 crisis, in view of limiting the damage of safety-critical cybersecurity incidents which have affected hospitals and health services providers.

Scope

The focus will be on improving the cybersecurity capabilities of healthcare and public health institutions across the EU, including cybersecurity services and products, skills and training, awareness raising, and exchange of information, and others. Cross-border solutions will be promoted where appropriate.

The types of tools intervention covered must include at least one of the following:

- Implementation of objectives and requirements under the NIS Directive in relation to the health sector;
- Support for the uptake in healthcare and public health institutions, and in particular SMEs, of software tools, methods, organisational and management practices, and training material dedicated to cybersecurity;
- Electronic ID (eID) and data management solutions contributing to data security in healthcare and public health institutions;
- Cybersecurity education, awareness and skills in healthcare and public health institutions.

Outcomes and deliverables

The funding will:

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide up to date tools to healthcare and public health institutions (in particular SMEs) to protect themselves against cyber threats.
- Contribute to data sharing in view to improve security collectively.

Type of action	SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries)
Indicative Budget	EUR 10 million
Indicative time of call opening	First call
Indicative duration of the action	Up to 24 months
Indicative budget per grant (EU contribution)	EUR 1 to 3 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.2 Support To Implementation Of Relevant EU Legislation

1.2.1 Deploying The Network Of National Coordination Centres With Member States

Objective

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 in a position 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.

Type of action	Simple grant (50% co-funding rate) to nominated beneficiaries
Indicative Budget	EUR 55 million
Indicative time of call opening	First and second call
Indicative duration of the action	24 months

Indicative budget per grant (EU contribution)	EUR 2 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.2.2 Cybersecurity Community support

Objective

In line with the regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, one project is foreseen to support community building in cybersecurity research, technology, and industrial policy at the EU level.

Scope

The community activities shall include activities such as:

- Support to Cybersecurity start-ups and scale-ups in all Member States, including with a view to attract investment to the EU;
- Support to the development and growth of an internal market in Cybersecurity products and services in the EU. Where relevant and appropriate, activities shall be in line with the JRC Cybersecurity taxonomy and Atlas[18];
- Support the European Cybersecurity Competence Centre and the Network of National Coordination Centres in fostering knowledge-sharing and networking between national, regional and local ecosystems specialised in cybersecurity;
- Support to education, training, and equality of opportunity in cybersecurity, in line with relevant actions promoted by organisations, including ENISA;
- Support awareness raising, including supports for national outreach and engagement to underpin cohesion of the Union in the field of cybersecurity.

All activities are to be carried out in support and under the supervision of the Commission and the European Cybersecurity Competence Centre once established.

Activities shall build on, complement, and provide additional value to the activities previously carried out in the framework of the contractual Public Private Partnership on Cybersecurity[19] and the four pilot projects on cybersecurity competence networks[20].

[18] https://cybersecurity-atlas.ec.europa.eu/ (Oct. 6, 2021)

[19] Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial, research and innovation between the EU and ECSO.

[20] CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

Activities shall be geographically balanced and inclusive towards the diversity of all members of the Community created by Regulation (EU) 2021/887, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

Activities shall take into account and enhance synergies with relevant European Digital Innovation Hubs created pursuant to article 16 of the Regulation establishing the Digital Europe Programme.

As this action is central to building a stronger cybersecurity ecosystem in Europe, this procurement falls under the essential security interest of the Union and will therefore be restricted.

Outcomes and deliverables

Strengthened Cybersecurity Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre.

Type of action	Procurement
Indicative Budget	EUR 3 million
Indicative year of procurement	2021
Indicative duration of the action	24 months
Indicative budget per grant (EU contribution)	EUR 3 million
Implementation	European Commission
Security	On the basis of article 12(5) of the Digital Europe Programme Regulation, 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 this document.

1.2.3 Supporting The NIS Directive Implementation And National Cybersecurity Strategies

Objective

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. It is a continuation of work currently supported under the CEF Telecom programme. 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[21].

Scope

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[22], 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 through the use of 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.

The support will target 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[23].

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

---

[21] 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.

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

[23] 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.

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

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

The action may support amongst other the continuation of the kind of cybersecurity activities funded through the CEF Telecom programme, building where relevant on the results from the CEF projects. Furthermore, synergies with actions from other relevant topics, e.g. 1.1 European "cyber-shield", should be explored.

Support will be provided amongst other for the on boarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of the NIS Directive and are potential users of the CEF Cybersecurity Core Service Platforms.

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.

The action will also lead to the interconnection of the centres in charge of guaranteeing the cybersecurity of the operator of important service.

Type of action	SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries)
Indicative Budget	EUR 20 million
Indicative time of call opening	Second call
Indicative duration of the action	36 months
Indicative budget per grant (EU contribution)	EUR 1 - 5 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

1.2.4 Testing and Certification Capabilities

Objective

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

Funding will be available for activities aiming to:

- Support capacity building for national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies including for thread-led 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), taking into account 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.
- Support SMEs to audit their infrastructure in view of improving their cybersecurity protection.
- Support actions in the area of standardisation.

Type of action

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.

The use of lump sums can be considered.

Type of action	Grant for Support to Third Parties
Indicative Budget	EUR 5 million
Indicative time of call opening	Second call
Indicative duration of the action	36 months
Indicative budget per grant (EU contribution)	EUR 0.5 to 1 million
Implementation	European Commission on behalf of the ECCC
Security	Call restricted on the basis of article 12(5) of the Digital Europe Programme Regulation

2 Programme Support Actions

Programme support actions aim at maximising the impact of the EU intervention. Horizontal actions will cover costs including preparation, evaluation, monitoring and studies. An amount of funding will be set aside to cover awareness and dissemination as it is crucial to effectively communicate about the value and benefits of the Digital Europe Programme. As an indicative list, programme support actions funded under this Work Programme might cover:

1. External expertise:

- The use of appointed independent experts for the evaluation of the project proposals and where appropriate, the monitoring of running projects;
- The use of individual independent experts to advise on, or support, the design and implementation of the underpinning policy.

2. Studies and other support actions:

- Events;
- Publications;
- Communication;
- Studies
- Other support measures, e.g. support to the Cyber Security Atlas.

Category of expenditure	**Indicative budget**
Proposals evaluation and project reviews	EUR 1.5 million
Studies	EUR 2.5 million
Other support measures	EUR 5 million
Total	EUR 9 million

3 Implementation

The programme counts with two main implementation modes: by using procurement and grants.

The different nature and specificities of the actions indicated in the previous chapters require distinctive implementation measures. Each of these will therefore be achieved through various implementation modes.

Proposers are strongly encouraged to follow green public procurement principles and take account of life cycle costs[24].

The implementation is articulated through different types of actions, which are indicated in each topic. More details on each type of action are described in Annex 2.

3.1 Procurement

Procurement actions will be carried out in compliance with the applicable EU public procurement rules. The procedures will be implemented either through direct calls for tenders or by using existing framework contracts. IT development and procurement activities will be carried out in compliance with European Commission's applicable IT governance rules.

3.2 Grants – Calls for Proposals

3.2.1 Evaluation Process

The evaluation of proposals will be based on the principles of transparency and equal treatment. It will be carried out by the Commission services together with the European Cybersecurity Industrial, Technology and Research Competence Centre and with the assistance of independent experts. Admissibility conditions

Proposals must be submitted before the call deadline and only through the means specified in the call for proposals. The call deadline is a deadline for receipt of proposals.

Proposals must be complete and contain all parts and mandatory annexes and supporting documents specified in the call for proposals. Incomplete proposals may be considered inadmissible.

Eligibility criteria

Proposals will be eligible if they are submitted by entities and/or consortiums compliant with the requirements set out in this Work Programme and the relevant call for proposals. Only proposals meeting the requirements of the eligibility criteria in the call for proposals will be evaluated further.

[24] http://ec.europa.eu/environment/gpp/index_en.htm (Oct. 6, 2021)

Exclusion criteria

Applicants which are subject to EU administrative sanctions (i.e. exclusion or financial penalty decision)[25] might be excluded from participation. Specific exclusion criteria will be listed in the call for proposals.

Financial and operational capacity

Each individual applicant must have stable and sufficient resources as well as the know-how and qualification to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects. Applicants must demonstrate their financial and operational capacity to carry out the proposed action.

Award criteria

The three sets of criteria are listed in Annex 1 of this Work Programme. Each of the eligible proposals will be evaluated against the award criteria. Proposals responding to a specific topic as defined in the previous chapters of this Work Programme will be evaluated both individually and comparatively. The comparative assessment of proposals will cover all proposals responding to the same topic.

Proposals that achieve a score greater than or equal to the threshold will be ranked within the objective. These rankings will determine the order of priority for funding. Following evaluation of award criteria, the Commission establishes a Selection Decision taking into account the scores and ranking of the proposals, the programme priorities and the available budget.

The coordinators of all submitted proposals will be informed in writing about the outcome of the evaluation for their proposal(s).

3.2.2 Selection Of Independent Experts For Evaluation And Reviews

The Commission and the Executive Agency will select independent experts to assist with the evaluation of proposals and with the review of project results as well as for other purposes where specific expertise might be required for implementation of the Programme. Experts are invited to apply using the mechanisms and tools provided for in the Horizon 2020 Framework Programme[26] and a list of experts appropriate to the requirements of the Digital Europe Programme and each addressed area will be established. Experts will be selected from this list on the basis of their ability to perform the tasks assigned to them, taking into account the thematic requirements of the topic, and with consideration of geographical and gender balance as well as the requirement to prevent and manage (potential) conflicts of interest.

3.2.3 Indicative Implementation Calendar

The indicative calendar for the implementation of the Digital Europe calls for proposals in the context of this Work Programme is shown in the table below. The table below does not prevent the opening of additional calls if needed.

[25] See article 136 of EU Financial Regulation 2018/1046.

26 http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html

More information about these calls will be available on: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

Table 5: Call timeline for topics in this Work Programme

Milestones	First call	Second call
Call Opening[27]	Q1 - 2022	Q3-2022
Deadline for submission[28]	Q2- 2022	Q4-2022
Evaluation	Q3 -2022	Q1-2023
Information to applicants on the outcome of the call	Q4 -2022	Q2-2023
Signature of contracts	Q1- 2023	Q3-2023

27 The Director-General responsible for the call may delay the publication and opening of the call by up to three months.

28 The Director-General responsible for the call may delay this deadline by up to three months.

4 Annexes

4.1 Annex 1 – Award Criteria For The Calls For Proposals

Proposals are evaluated and scored against award criteria set out for each topic in the call document. The general award criteria for the Digital Europe calls are as follows:

1. Relevance:

- Alignment with the objectives and activities as described in the call for proposals
- 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*

* This might not be applicable to all topics

2. Implementation

- Maturity of the project
- Soundness of the implementation plan and efficient use of resources
- Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

3. Impact

- Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, when 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*

*This might not be applicable to all topics and in only exceptional occasions and for duly justified reasons may not be evaluated (see specific topic conditions in the call for proposals).

4.2 Annex 2 – Types of action to be implemented through grants

The descriptions below of the types of actions to be implemented through grants under the Digital Europe Programme is indicative and should help the (potential) applicants to understand the expectation in each type of action. The call text will define the objectives and scope of the action in more detail.

Simple Grants

Description: The simple grants 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% of total eligible costs for all beneficiaries.

SME support actions

Description: Type of action primarily consisting of activities directly aiming at supporting SMEs involved in building up and the deployment of the digital capacities. This action can also be used if SME needs to be in the consortium and make investments to access the digital capacities.
Funding rate: 50% of total eligible costs except for SMEs where a rate of 75% applies.

Coordination and support actions (CSA):

Description: Small type of action with the primary goal to promote cooperation and/or promote support to 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. CSA may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100% of eligible costs.

Grant for financial support

Description: Actions with 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 V 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% of eligible costs for the consortium, co-financing of 50% of total eligible costs by the supported third party.

4.3 Annex 3 - Implementation Of Article 12(5)

As indicated in this document, as will be additionally detailed in the call document, and if justified for security reasons, an action falling under specific objective 3 can exclude the participation of legal entities controlled by a third country[29] (including those established in the EU territory but controlled by a third country or by a third country legal entity).

The assessment of the foreign control will be addressed during the eligibility phase of the evaluation of proposals. For this, participants will be requested to fill in a self-assessment questionnaire to determine their control status during proposal submission. They will also be requested to submit supporting documents in order for the Commission to determine that the entities are not controlled by a third country.

In the particular case of topics 1.1.4 (Uptake of Innovative Cybersecurity Solutions) and 1.2.2 (Cybersecurity community support), the legal entities judged to be controlled by a third country can participate in the respective call for proposals and call for tenders, provided that they comply with certain conditions set out below. Those participants will be asked for guarantees approved by the eligible country in which they are established. The validity of these guarantees will be later assessed by the European Commission.

Conditions for foreign controlled entities in the context of topics 1.1.4 and 1.2.2

The foreign controlled applicant shall be required to provide information demonstrating that:

(a) control over the applicant's corporate structure and decision-making process is not exercised in a manner that restrains or restricts in any way its ability to perform and complete the action;

(b) the access by non-eligible third countries or by non-eligible third country entities to classified and non-classified sensitive information[30] relating to the action will be prevented;

(c) the persons involved in the action will have national security clearance issued by a Member State where appropriate;

(d) the results of the action shall remain within the beneficiary and shall not be subject to control or restrictions by non-eligible third countries or other non-eligible third country entities during the action and for a specified period after its completion.

(e) For applicants established in the EU and controlled from a third country and established in Associated Countries, that are not subject to export restrictions to EU Member States on results,

[29] See article 12(5) of the Digital Europe Programme Regulation

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

technologies, services and products developed under the project for at least 4 years after the end of the action, in order to ensure the security of supply.

More information about the procedure, the conditions and the guarantees will be detailed in the call documents and the online manual in the EU Funding & Tenders portal.

More information will be published in the Funding and tenders portal and in the procurement-related documents.