EUROPEAN
COMMISSION

Brussels, 24.3.2023
C(2023) 1862 final

ANNEX 2

ANNEX

to the

Commission Implementing Decision

on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024 and amending the Commission Implementing Decision C(2021) 7914 on the adoption of the multiannual work programme for 2021-2022

DIGITAL EUROPE
Cybersecurity

Work Programme 2023-2024

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 we interact, communicate and educate ourselves. The critical role of digital technologies and infrastructures, and the interdependencies in our societies and economies, have recently been demonstrated by disruptive events such as the COVID-19 crisis and Russia's war of aggression against Ukraine. These crises have confirmed how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world. Malicious cyber activities not only threaten our economies but also our way of life, our freedoms and values, and even try to undermine the cohesion and functioning of our democracy in Europe.

In December 2020, the Commission and the High Representative presented the EU's Cybersecurity Strategy for the Digital Decade[1], 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 networks, 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.[2] The efforts needed to achieve the aforementioned goals are not limited to Research and Development.

Europe should indeed strive for more technological sovereignty. A pillar of the EU cybersecurity strategy is the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) with the Network of National Coordination Centres (NCCs)[3]. The ECCC is EU's initiative to support innovation and industrial policy in cybersecurity. The ECCC will develop and implement, with Member States and countries associated to Specific Objective 3 of the Digital Europe Programme, industry and the academic community, a common agenda for cybersecurity technology development and deployment in strategic areas. The NCCs and the ECCC together will enhance the EU's technological sovereignty, supporting projects in critical areas and benefiting, in particular, SMEs.

The Digital Europe Programme supports the co-investment strategy foreseen by Regulation (EU) 2021/887 establishing the ECCC.

The second Work Programme (WP) Cybersecurity of the Digital Europe Programme 2023-2024 responds to a two-fold challenge. It ensures the continuation and evolution of actions started in the first Work Programme Cybersecurity 2021-2022 (notably the support for National Coordination Centres), while simultaneously introducing actions that follow the priorities of the EU to further develop its cybersecurity capabilities and enhance its resilience in the context of the EU Cybersecurity Strategy.

This document sets out the Cybersecurity WP for part of the actions to be implemented in 2023 and 2024 under Specific Objective 3: Cybersecurity and Trust of the Digital Europe Programme. It uses as

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

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

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

a reference point the Annex 1 of the Regulation (EU) 2021/694 of the European Parliament and of the Council.[4]

For the year 2023 the WP contains descriptions of scope, goals and deliverables for each action; while for 2024 the objectives and expected results are to be articulated at the level of the specific objectives, indicating probable actions and more general description and indication of the type of action. This is to allow sufficient flexibility of the programme in response to the results of the actions achieved in the first two years of the Programme, as described in the WP Cybersecurity 2021-2022.

Participation to the calls funded under this WP will be subject to the provisions of Article 12.5 of Regulation (EU) 2021/694. Calls for proposals and calls for tenders funded under this WP will be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States. (Appendix 3).[5]

THE DIGITAL EUROPE PROGRAMME OBJECTIVES

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

The Digital Europe Programme also targets upskilling and reskilling to provide a workforce for these advanced digital technologies. It supports industry, small and medium-sized enterprises (SMEs), and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs (EDIH).

Actions in this work programme will in particular support the objectives indicated below.

- Support joint actions in order to create an advanced (state of the art) threat detection and cyber incident analysis ecosystem by building capacities of **Security Operation Centres (SOCs)**.
- Contribute to improving the prevention, detection, analysis and capability to learn and respond to cyber threats and incidents by providing additional means and better interplay amongst cyber communities[6] to support preparedness (ex-ante), and response (ex-post) to large-scale cybersecurity incidents via **Cybersecurity Emergency Mechanism.** This has two components: one on **Incident Response Support**, one on **preparedness and mutual assistance**. The one on Incident Response Support is part of the Digital Europe Programme's Main WP. The one on preparedness and mutual assistance is part of this WP.
- Support cybersecurity capacity building at national and, where relevant, regional and local levels through **National Coordination Centres** which will aim at fostering cross-border

[4] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1–34).

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

[6] E.g., NIS authorities, CSIRTs; law enforcement cyber units and judicial authorities; cyber diplomacy; and cyber defence.

cooperation and at the preparation of joint actions as defined in the Regulation (EU) 2021/887.

- Support the **industry with a strong focus on helping SMEs and start-ups in** complying with **regulatory requirements**, especially the NIS2[7] implementation or requirements concerning the proposed Cyber Resilience Act (Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020)[8].

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.

This Work Programme does not stand by itself in pursuing these objectives. Rather, it is complemented with actions in the Main Digital Europe WP. In addition to before mentioned action on Incident Response Support (Section 3 of the Main WP), the following actions are designed to reinforce EU's advanced cybersecurity capacities in the area of education and investments.

- The Cybersecurity Skills Academy will constitute an EU umbrella, integrating various activities such as development of training programmes and universal curricula in order to increase their visibility, accessibility and impact on the market (Section 4.3 of the Main WP).
- The implementation of the Investment Platform for Strategic Digital Technologies under the InvestEU program will provide improved dedicated financial support to innovative digital start-ups and SMEs at all stages of their development for strategic digital technologies, with a special focus on cybersecurity (Section 7.1 of the Main WP).

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 and long-term economic costs and make Europe susceptible to undue foreign influence. Cybersecurity incidents can be either accidental or 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.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80–152).

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

All actions under this WP 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 in particular supply-chain attacks.

The participation on non-EU entities could lead to highly sensitive information about security risks and incidents being subject to legislation that obliges the non-EU parties to provide this information to non-EU governments. Non-EU participants could also be more susceptible to pressure from non-EU governments to divulge such information.

This means that in order to protect the essential security interests of the Union, the implementation of cybersecurity topics 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 this particular criticality, participation to the calls funded under this WP will be subject to the provisions of Article 12.5 of the Regulation (EU) 2021/694, as indicated in each topic. Those calls for proposals and calls for tenders shall be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States. Further information is included in point 4.3 Appendix 3 - Implementation of Article 12(5).

INDICATIVE BUDGET AND IMPLEMENTATION

Digital Europe is implemented by means of multiannual Work Programmes. This Work Programme covers Cybersecurity topics that will be implemented by the ECCC.

Until the ECCC has the capacity to implement its own budget, the European Commission will implement the actions in direct management on behalf of the ECCC. The budget for Cybersecurity actions covered by this Work Programme is EUR 375 million, out of which EUR 161 million is to be distributed in 2023, as follows:

- EUR 84 million for actions related to building capacities of Security Operation Centres,
- EUR 35 million for actions in relations to the Cybersecurity Emergency Mechanism component on preparedness and mutual assistance,
- EUR 3 million for coordination between the cybersecurity civilian and defence Spheres,
- EUR 3 million for standardisation,
- EUR 30 million for support for implementation of EU legislation on cybersecurity and National Cybersecurity Strategies,
- EUR 6 million for programme support actions, including evaluations and reviews.

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

Year	Budget line	Total per budget line, per year (in million EUR)
2023	**Specific Objective 3 (02 04 01 11)**	161
2024	**Specific Objective 3 (02 04 01 11)**	214
	Grand Total	375

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

LINKS TO OTHER PROGRAMMES AND CO-INVESTMENTS

Most actions foreseen in the Digital Europe Programme require co-investments from the public and private sectors. The modes of these co-investments are described in the relevant parts of the various work programmes.

As far as possible funding support from other EU instruments to actions in this WP is concerned, alternating or cumulative funding may be considered, provided that such funding is in line with the fund-specific regulations of the funding instruments in question, and in line with the objectives of the relevant programmes. Relevant provisions of the Regulation (EU, Euratom) 2018/1046 need to be respected[9], in no circumstances the same costs shall be financed twice by the EU budget (prohibition of double funding). Funding from cohesion policy programmes can fall under EU State aid rules when the beneficiaries are undertakings. In such cases, the funding must be compatible with EU State aid rules.

An alternating/sequenced funding occurs when each instrument finances a different part of the operation/action, or finances successive parts. It requires a split of an operation/action in two different parts. Separate grant agreements are required, applying the rules of the funding instruments respectively. Coordination is required to avoid double funding, ensuring the separation of parts/activities. Expenditure used for a reimbursement request for one instrument shall not be declared for support from another Fund or Union instrument. Activities financed under separate instruments have to be clearly differentiated.

Cumulative funding means that an action receives support from more than one fund, programme or instrument (including both shared and directly managed funds). Two grant agreements are required, applying the rules of each of the funding instruments respectively. Upfront coordination is required to avoid double funding by coordinating the funding rates which in combination cannot go over 100% of the eligible costs. A number of steps starting from preparation, through linking of actions, grant signatures all the way to reporting and payments need to be followed. The draft Commission Notice

[9] In particular the Article (191) Principle of non-cumulative award and prohibition of double funding

on Synergies between Horizon Europe and the ERDF programmes[10] elaborates on new opportunities to maximise synergies between Horizon Europe and the European Regional Development Fund, including on cumulative funding. An example on how such cumulative funding is applied to Digital Europe Programme and cohesion policy funds is outlined in the Annex 2 of the Notice.

In the specific case of cumulative funding between Digital Europe Programme and Recovery and Resilience facility, the Section 3 of the Guidance document to Member States[11] confirms that support from Digital Europe Programme can also be combined with the Recovery and Resilience Facility, provided that such support does not cover the same cost (for example by clearly distinguishing what is to be covered by each funding source). Member States shall ensure the effective and efficient functioning of such synergies, through a consistent and harmonised approach of all involved authorities and close coordination between all public actors is needed.

Below is an outline of actions for which cumulative funding could be considered. However, support from multiple funding sources is in all cases subject to decisions of the authorities managing the funding instruments.

Table 2: Actions for which cumulative funding could be considered

Topics in the Work Programme	**DIGITAL Funding rate**
Security Operation Centres	75% for joint procurement and 50% for grants
Cybersecurity Emergency Mechanism	50% procurement
Deploying the Network of National Coordination Centres with Member States	50%

MULTI COUNTRY PROJECTS AND THE EUROPEAN DIGITAL INFRASTRUCTURE CONSORTIA

As part of the 2030 Policy programme "Path to the Digital Decade"[12], the Commission has introduced the concept of Multi-Country Projects (MCPs). MCPs are large-scale deployment and capacity-building projects for the digital transformation of the Union, facilitating the achievement of the Digital Decade objectives and targets[13]. They channel coordinated investments between the EU, Member States and private stakeholders to, i.a., enable digital infrastructure projects that one single Member State could not deploy on its own. They help reinforce the Union's technology excellence and industrial competitiveness in critical technologies; support an interconnected, interoperable and

[10] Synergies between Horizon Europe and ERDF programmes (2022) https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/synergies-guidance-out-2022-07-06_en

[11] SWD (2021) 12 final

[12] COM/2021/574 final

[13] Digital Compass: the European way for the Digital Decade: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

secure Digital Single Market and address strategic vulnerabilities and dependencies of the Union along the digital supply chain. This means that setting up a MCP in a relevant area fits the objectives of the Digital Europe programme and provides additional incentives for Member States and companies to work together to build pan-European digital infrastructures.

A number of areas of MCPs are in the scope of the Digital Europe programme and are receiving funding under the Digital Europe Main WP 2021-22 and Cybersecurity WP.[14] The Multi-Country Project in this WP is Deploying a network of security operations centres.

In order to facilitate the set-up and enable speedy implementation of MCPs for which a specific set of features is necessary, the Commission also introduced a new instrument, the European Digital Infrastructure Consortium (EDIC). The legal framework of EDICs is closely modelled on the existing and successful one in the area of research activities, namely the European Research Infrastructure Consortium (ERIC), but for area beyond research and with limited changes to increase flexibility in the implementation, such as enabling private parties to participate in the EDIC as members, and making sure projects remain open to all interested Member States.

Only the Member States may submit an application to form an EDIC. Where Member States progress sufficiently with their applications for EDICs, this option should be supported to the greatest extent possible, to attract further funding for large-scale MCPs. Once an EDIC is formally established, it may make a proposal in response to a formal Call for proposals (like any other proposer) applying the rules contained in the relevant Call document. Depending on the interest in specific EDICs shown by the Member States, an amendment to this WP could be made to strengthen the link of an EDIC with any specific existing or new action. At the time of the preparation of this WP, no EDICs in relation to the actions described in this WP were in preparation.

CLIMATE AND BIO-DIVERSITY

Digital tools have the potential to contribute to climate: AI can via interconnected technologies be an enabler for low-carbon smart cities and ensure that energy consumption is efficient, digital services remove the need for physical presence, data space can provide data to organisations that can help them improve the efficiency, energy consumption in specific sectors. Cybersecurity infrastructures and tools supported by this work programme aim to support the use of such technologies by making them safe and thereby enabling their wider adoption. This ranges from consumer products to the protection of more efficient critical infrastructures and essential services, up to the capacity of organisations to detect cyber threats and to respond to attacks in an efficient manner and to ensure that authorities can be prepared for them. It will help Member States work together to be better prepared for large scale cyber-attacks. While cybersecurity is not aimed at, for instance, reducing the energy consumption of these tools, it is a precondition for using many technologies that do exactly this.

[14] The initial list of areas of activity for Multi-Country projects, as per 2030 policy programme "Path to the Digital Decade" Annex is listed in Annex 4 (Section 9.4) of the Main WP 2023-2024.

As for biodiversity, cybersecurity does not directly contribute to the conservation and restoration of biodiversity (ecosystems, species, and genetic diversity), the maintenance of related ecosystem services; the sustainable use and management of biodiversity and ecosystems (including activities within agriculture, forestry, fisheries and other sectors); or the fair and equitable sharing of the benefits of the utilisation of genetic resources.

CALLS STRUCTURE AND PLANNING

Calls for Proposals

Table 3: List of topics in the First set of calls for proposals (grants and procurement) under this Work Programme (2023) with a common deadline

Area	Topics in the Work Programme	Indicative budget (in million EUR)
Security Operation Centres	Call for Expression of Interest on National SOCs	50
	Call for Expression of Interest on Cross-Border SOC Platforms	30
	Strengthening the SOC ecosystem	4
Cybersecurity Emergency Mechanism	Preparedness Support and Mutual Assistance	35
	Coordination Between the Cybersecurity Civilian and Defence Spheres	3
	Standardisation in the Area of Cybersecurity	3
	Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies	30
	Total	**155**

The table with the list of indicative topics for 2024 is included under Section 3.2.3 on Indicative implementation calendar.

Contents

1 Deployment actions in the area of cybersecurity

1.1 Security Operation Centres

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

The EU Cybersecurity Strategy proposes to build, strengthen, and interconnect, across the European Union, Security Operation Centres (SOCs) and Cyber Threat Intelligence (CTI) capabilities (monitoring, detection and analysis), with the aim to support the detection and prevention of cyber threats and the provision of timely warnings to authorities and all relevant stakeholders. Such cyber security capabilities are typically ensured by SOCs in combination with Computer Emergency Response Teams / Computer Security Incident Response Teams (CERTs/CSIRTs), with the support of external, specialised sources of intelligence on cyber threats.

To implement this strategy, the previous DIGITAL work programme (2021-2022) included actions concerning Capacity Building of SOCs. This work programme aims at strengthening EU actions by supporting the creation of National SOCs, and networking them at European and EU level via Cross-Border SOCs and coordinating their activities to create a stronger SOC ecosystem, also comprising of local and regional, private and public security centres for both horizontal and vertical sectors.

These SOC platforms, that will be equipped with state-of-the-art digital technologies and tools to be continuously kept up to date, should in particular enable the exchange and analysis of data on cybersecurity threats from various sources, on a large-scale and in a trusted environment.

The objective will be to support joint actions to create an advanced (state-of-the-art) threat detection and cyber early warning ecosystem. This will allow to reinforce capacities through the coordination of actions on collective knowledge and data sources, bringing together data from multiple sources and expanding cybersecurity threat intelligence. By fostering common and interoperable infrastructures, this will make it possible to more efficiently and more rapidly share and correlate the signals detected, thus enabling a better situational awareness and a more rapid and effective reaction. The actions in this WP are focussed along three strands.

- Building and strengthening National SOCs, which will play a key role as a hub or gateway to other SOCs at national level.
- Capacity building for cross-border SOC platforms.
- Strengthening the SOC ecosystem with cross cutting actions and support for local, regional or vertical SOCs.

The Union financial contribution shall cover up to 75% of the acquisition costs under joint procurement, for which a hosting and usage agreement will be concluded. Up to 50% of the running costs of National or Cross-Border SOCs may be covered by a complementing grant, provided necessary requirements are met. The remaining total cost of ownership of the national and cross-border SOCs shall be covered by the Participating States in the hosting consortium.

1.1.1 National SOCs

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

Objective

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

Scope

The aim is capacity building for new or existing National SOCs, e.g., equipment, tools, data feeds, as well as costs related to data analysis, interconnection with Cross-Border SOC platforms, etc. This can include for example automation, analysis and correlation tools and data feeds (covering CTI at different levels ranging from field data to (Security Information and Event Management) SIEMs data to higher level CTI). National SOCs should also leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context. This also includes the use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information. The operations should be built upon live network data. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

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

Another key role for National SOCs is knowledge transfer, such as training of cybersecurity analysts. For example, the staff of SOCs dealing with critical infrastructures plays a key role and should benefit from the knowledge and experience acquired by or concentrated in National SOCs.

National SOCs must share information with other SOCs in a mutually beneficial exchange of information, and commit to become part of a cross-border SOC platform within the next 2-3 years, with a view to exchanging information with other National SOCs.

To achieve this aim, the following actions are foreseen:

- A call for expression of interest[15] will be launched to select entities in Member States that provide the necessary facilities to host and operate National SOCs. The call for expression of interest will also build up the planning and design of necessary tools and infrastructures.
- Building on this call for expression of interest, the ECCC and the selected entities will jointly acquire through procurement capacities needed for the National SOCs, including the necessary IT tools, infrastructure and associated services. This includes advanced tools and infrastructures to securely share and analyse large data sets and threat intelligence.
- Applicants may request a grant to fund running costs and other costs of the National SOCs.

Deliverables

- World-class National SOCs across the Union, strengthened with state-of-the-art technology, acting as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.
- Threat intelligence and situational awareness capabilities and capacity building supporting strengthened collaboration between cybersecurity actors, including private and public actors.

Type of action	Call for Expression of Interest (Joint procurement with Member States)
Indicative budget	EUR 35 million. The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 1.1.1 based on the amounts requested in the submissions received.
Indicative call planning[16]	First set of calls
Indicative duration of the action	2 years
Implementation	ECCC
Type of beneficiaries	In particular public bodies acting as National SOCs, as identified by Member States
Security	Call for grants and procurement are restricted on the basis of article 12(5) of the Regulation (EU) 2021/694. * Further explanation on Grants and Procurement

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

[16] For indicative timing see Table 4.

	conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

Type of action	Simple Grants
Indicative budget	EUR 15 million. The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 1.1.1 based on the amounts requested in the submissions received.
Indicative call planning[17]	First set of calls
Indicative duration of the action	2 years
Implementation	ECCC
Type of beneficiaries	Successful Consortia of the Call for Expression of Interest for National SOCs
Security	Call for grants and procurement are restricted on the basis of article 12(5) of the Regulation (EU) 2021/694. * Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

1.1.2 Cross-Border SOC Platforms

Cross-border SOC platforms are collaborative platforms where National SOCs collaborate in a cross-border context. The objective of such platforms is to strengthen capacities to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention capabilities in a trusted environment.

Objective

The general objective of cross-border SOC platforms is to strengthen capacities to analyse, detect and prevent cyber threats and to support the production of high-quality intelligence on cyber threats, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and

[17] For indicative timing see Table 4.

prevention capabilities in a trusted environment. They should provide new additional capacity building upon and complementing existing SOCs and CSIRTs and other relevant actors.

Scope

Cross-border SOC platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI, supporting the development of better performing data analytics, detection, and response tools, through the pooling of larger amounts of data, including new data generated internally by the consortia members.

The platforms should act as a central point allowing for broader pooling of relevant data and CTI, enable the spreading of threat information on a large scale and among a large and diverse set of actors (e.g., CERTs/CSIRTs, ISACs, operators of critical infrastructures).

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

The platforms will support common situational awareness and effective crisis management and response by providing relevant information to networks and entities responsible for cybersecurity operational cooperation and crisis management at Union level, without undue delay, where they obtain information related to an ongoing large-scale, cross-border incident, or to a major threat or a major vulnerability likely to have significant cross-border impacts or significant impacts on services and activities falling within the scope of the Directive (EU) 2022/2555[18].

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

To achieve this aim the following actions are foreseen.

- A call for expression of interest[19] 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). The call for expression of interest will also build up the planning and design of necessary tools and infrastructures.
- Building on this call for expression of interest, the ECCC and the selected entities will engage in a joint procurement to acquire capacities needed for the cross-border SOC platforms, including the necessary IT tools, infrastructure and associated services. This includes

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

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

advanced tools and infrastructures to securely share and analyse large data sets and threat intelligence among the participating National SOCs.

- Applicants may request a grant to fund running costs and other costs of the cross-border SOC platforms.

Deliverables

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

Type of action	Call for Expression of Interest (Joint procurement with Member States)
Indicative budget	EUR 20 million. The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 1.1.2 based on the amounts requested in the submissions received.
Indicative call planning[20]	First set of calls
Indicative duration of the action	2 years
Implementation	ECCC
Type of beneficiaries	In particular National SOCs, as identified by Member States
Security	Call for grants and procurement are restricted on the basis of article 12(5) of the Regulation (EU) 2021/694. * Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

Type of action	Simple Grants

[20] For indicative timing see Table 4.

Indicative budget	EUR 10 million. The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 1.1.2 based on the amounts requested in the submissions received.
Indicative call planning[21]	First set of calls
Indicative duration of the action	2 years
Implementation	ECCC
Type of beneficiaries	Successful Consortia of the Call for Expression of Interest for National SOCs
Security	Call for grants and procurement are restricted on the basis of article 12(5) of the Regulation (EU) 2021/694. * Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

1.1.3 Strengthening the SOC ecosystem

Objective

This topic complements other actions in this and the previous Work Programme, which are building up National SOCs and Cross-Border SOC platforms. It will contribute to local SOCs which are linked to National SOCs, and to a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms, leading to an increased data sharing and better detection capability for cyber threats. This should in particular foster interoperability, identifying what data can be shared, how this is shared and in what format, requirements and sharing agreements, and ways to enable better exchange. Links to the actions funded under the Cyber Academy (in the main Digital Europe work programme) can also be envisaged.

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

Additionally, Cross-Border SOC Platforms will develop a comprehensive governance framework, with for example enrolment conditions and vetting procedures. The aim is to foster discussion between such platforms, sharing best practices and identifying opportunities for collaboration.

[21] For indicative timing see Table 4.

One Coordination and support action grant will be selected, bringing together the largest possible network of National and Cross-Border SOCs.

Scope

Actions should address the following:

- Activities that foster the collaboration and interconnection between Cross-Border SOC platforms and National SOCs, as well as fostering the link between National SOCs and other SOCs at national level. This concerns in particular improving and developing solutions for interoperability, such as common data formats, taxonomies and exchange mechanisms, and collaborative approaches such as the adoption of common tools and the creation of data lakes.
- Actions that support the cooperation and coordination of Cross-Border SOC platforms, both between different Cross-Border SOC platforms, and with relation to national SOCs and other SOCs.

Deliverables

- White papers on technical coordination and interconnection support platforms.
- Organization of events, workshops, stakeholder consultations, and production of white papers, architectural designs, which strengthen the links within the SOC ecosystem.
- Organization of events, workshops, stakeholder consultations, and production of white papers, architectural designs, which support the cooperation and coordination within and across Cross-Border SOC platforms.

Type of action	Coordination and support action grant
Indicative budget	EUR 4 million
Indicative call planning	First set of calls
Indicative duration of the action	3 years
Implementation	ECCC
Type of beneficiaries	National SOCs and Cross-Border SOCs Platforms
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

1.2 Cybersecurity Emergency Mechanism

In March 2022, the EU ministers in charge of telecommunications unanimously called for the implementation of a new Emergency Fund for Cybersecurity in view of the elevated threat of malicious cyber activities and acknowledging that the current geopolitical landscape and its impact in

the cyberspace call for the EU to fully prepare to face large-scale cyberattacks and strengthen its capabilities in cybersecurity.

In the Joint Communication on EU Policy Cyber-defence, it was announced that as part of the EU Cyber Solidarity initiative, the Commission is preparing actions to strengthen preparedness and response actions across the EU. This work programme will support the EU Cyber Solidarity initiative through the testing of essential entities and the gradual set-up of an EU-level cyber reserve with services from trusted private providers that would be ready to intervene at Member States' request in cases of significant cross-border incidents.

This includes the testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments – building on actions already initiated by the Commission together with ENISA - as well as coordinated incident response actions to mitigate the impact of serious incidents, to handle digital evidence in forensically sound manner, to support immediate recovery and/or restore the functioning of essential services.

The mechanism will directly contribute by providing additional means to support **preparedness (ex-ante)**, and **response (ex-post)** to large-scale cybersecurity incidents.

The Cybersecurity Emergency Mechanism has two components: one on **Incident Response Support** one on **preparedness and mutual assistance**. The one on Incident Response Support is part of DIGITAL's Main Work Programme. The one on preparedness and mutual assistance is mostly covered in this DIGITAL's Cybersecurity Work Programme, and it is described below.

1.2.1 Preparedness Support and Mutual Assistance

Objective

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

The mechanism should also support mutual assistance between Member States for both preparedness and incident response actions.

Scope

The provision of **preparedness support services** (ex-ante) shall include activities listed below:

a) Support for testing of essential entities operating critical infrastructure for potential vulnerabilities.

- Development of **penetration testing** scenarios for MS cybersecurity infrastructure (including infrastructure of Operators of Essential Services, Digital Service Providers and Governmental entities). The proposed scenarios should cover Networks, Applications, Virtualization solutions, Cloud solutions, Industrial Control systems, and IoT.
- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.

- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant**.**
- Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities.

b) Support for threat assessment and risk assessment.

- Threat Assessment process implementation and life cycle.
- Customised risk scenarios analysis.

c) Risk monitoring service.

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

Preparedness actions should benefit entities in NIS2 (Directive (EU) 2022/2555) sectors (e.g., energy, transport, banking, …) and entities in other relevant sectors, as well as including SMEs and start-ups. Also within scope are actions for mutual assistance among Member States, i.e., tailored and targeted short-term assistance upon request and depending on the specific needs arising from an incident.

Deliverables:

- preparedness support services
- threat assessment and risk assessment services
- risk monitoring services
- mutual assistance among Member States

Type of action	Grant for Financial Support
Indicative budget	EUR 35 million
Indicative call planning	First set of calls
Indicative duration of the action	2 years
Implementation	ECCC
Type of beneficiaries	All entities
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

1.3 Coordination Between the Cybersecurity Civilian and Defence Spheres

Objective

The objective is to enhance exchange and coordination between the cybersecurity civilian[22] and defence spheres. This should in particular foster synergies between cybersecurity actions in Horizon Europe, Digital Europe and defence related actions carried out by the Union through its bodies and programmes, such as the European Defence Agency and the European Defence Fund.

Scope

The aim is to organise activities that bring foster exchange with regards to cybersecurity technologies that have relevance in both civilian and defence context: meetings, workshops and collaborative activities between stakeholders of the civil and defence communities, addressing all stakeholders (academic, SMEs, industry, public authorities, etc.).

Deliverables

- Concrete activities such as discussions, meetings, white papers, workshops, which strengthen the links between the cybersecurity civilian and defence spheres.
- Synergies between these communities, such as common activities to exchange know-how and information.

Type of action	Coordination and support action grant
Indicative budget	EUR 3 million
Indicative call planning	First set of calls
Indicative duration of the action	3 years
Implementation	ECCC
Type of beneficiaries	All entities
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

1.4 Standardisation in the Area of Cybersecurity

Objective

The objective of this topic is to support further standardisation in the area of cybersecurity, notably in view of the implementation of the proposed Regulation on the Cyber Resilience Act (CRA)[23], in

[22] Including CSIRTs, law enforcement and cyber diplomacy communities

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

particular with a view to improving the awareness and engage stakeholders in such standardisation work.

Scope

The aim is to ensure wide stakeholder participation in standardisation activities in the area of cybersecurity, and in particular in relation to development of harmonized standards facilitating the implementation of the Cyber Resilience Act. This can be in the form of meetings, workshops and collaborative activities, involving the private as well as the public sector.

The Cyber Resilience Act (CRA) proposal aims to improve the internal market's functioning by mandating that all products with digital elements (hardware and software) will only be made available on the market if they meet specific essential cybersecurity requirements. In order to facilitate the implementation of the CRA, harmonised standards would be developed, which, if followed, would trigger the presumption of conformity with the CRA essential cybersecurity requirements to which they correspond. This will be complementary to actions by the National Coordination Centres, which will play a key role in reducing negative cross-border spillovers and subsequent costs to society to mitigate the risks associated with non-secure products.

Deliverables

- Organization of events, workshops, stakeholder consultations, and production of white papers, all fostering the development of harmonised standards and conformity with requirements stemming from above mentioned legislative framework.
- Support for participation of relevant European experts in European and international cybersecurity standardization fora.

Type of action	Coordination and support action grant
Indicative budget	EUR 3 million
Indicative call planning	First set of calls
Indicative duration of the action	3 years
Implementation	ECCC
Type of beneficiaries	All entities
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

1.5 Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies

Objective

The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555)[24], the Cybersecurity Act[25] and the proposed Cyber Resilience Act[26], and the Directive on attacks against information systems (Directive 2013/40)[27]. It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous Digital Work Programme.

In addition, the action also aims at improving industrial and market readiness for the cybersecurity requirements set in the proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act bolstering cybersecurity rules to ensure more secure hardware and software products.

Proposals should contribute to achieving at least one of 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.
- Better reporting of cyber-attacks to law enforcement authorities in line with the Directive on attacks against information systems.
- Improved security of network and information systems in the EU.
- More alignment of Member States' implementations of NIS2 (Directive (EU) 2022/2555).
- Support cybersecurity certification in line with the Cybersecurity Act.

Scope

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

- Implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents.
- Collaboration, communication, awareness-raising activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).

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

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

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

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

- Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.
- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.
- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.
- Enable businesses across all sectors and consumers to use products with digital elements securely.
- Support to Cybersecurity certification, including support to national cyber authorities and other relevant stakeholders, such as SMEs.

The support will target relevant Member State competent authorities, which play a central role in the implementation of NIS2 (Directive (EU) 2022/2555), as well as other actors with the scope of this Directive.

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.

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 NIS2 (Directive (EU) 2022/2555) and are potential users of the CEF Cybersecurity Core Service Platforms.

The action also supports industry, with a particular focus on start-ups and SMEs, to seize the industrial and market uptake opportunities given by the proposed Cyber Resilient Act and Cybersecurity Act.

Deliverables

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organization of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions in the area of certification.

Type of action	Simple grant
Indicative budget	EUR 30 million
Indicative call planning	First set of calls
Indicative duration of the action	36 months
Indicative budget per grant (EU contribution)	EUR 1 - 2 million
Implementation	ECCC
Type of beneficiaries	All entities
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

Actions in 2024

- **Continuation of the action Cross-Border SOC Platforms (Section 1.1.2): Advanced Key Technologies for SOCs platforms**

  Objective

  This topic complements other actions in this and the previous WP, which are building up National SOCs and Cross-Border SOC platforms. It will contribute to improve the capabilities SOC platforms to mature, test, validate and deploy tools based on key technologies such as AI and Machine Learning, HPC enhancing capacities for data sharing and analytics, and other relevant cybersecurity functions to boost the detection and correlation of features across of Cross-Border platforms.

  The topic will also contribute to the further development and use of advanced data analytics methods and tools in support of SOCs operations. Such AI/ML tools can be developed also for testing the defence capabilities of Cross-Border SOCs and find vulnerabilities (i.e. penetration tests).

  Deliverables:

  - Tools based on novel technologies deployed in SOCs and Cross-Border SOC platforms
  - Increase capabilities, for example in the area of data analytics and capability testing

  Indicative type of action: Simple Grant
  Indicative type of implementation: ECCC
  Type of beneficiaries: SOCs and Cross-Border SOCs Platforms

- **Continuation of the action Preparedness Support and Mutual Assistance** (Section 1.2.1)

Objective

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

The mechanism should also support mutual assistance between Member States for both preparedness and incident response actions.

Deliverables:

- preparedness support services
- threat assessment and risk assessment services
- risk monitoring services
- mutual assistance among Member States

Indicative type of action: Grant for Financial Support
Indicative type of implementation: ECCC
Type of beneficiaries: all entities

- **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 can also support priority areas such as the implementation of EU legislation ((Directive (EU) 2022/2555, the proposed Cyber Resilience Act[28], Cybersecurity Act[29]).

Deliverables

- Operation of National Coordination Centres in Member States
- Support for the Cyber Resilience Act, the NIS directive and future legislation

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

[29] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15–69).

- Support for the resilience of European infrastructures, supply chains
- Awareness raising and dissemination of training material

Indicative type of action: Simple Grant
Indicative type of implementation: ECCC
Type of beneficiaries: National Coordination Centres

- **Continuation of the action Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies** (Section 1.5)

Objective

The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555)[30], the Cybersecurity Act[31] and the proposed Cyber Resilience Act[32], and the Directive on attacks against information systems (Directive 2013/40)[33]. The action also aims at improving industrial and market readiness for the cybersecurity requirements set in the proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act bolstering cybersecurity rules to ensure more secure hardware and software products.

Deliverables:

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organization of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions in the area of certification.

Indicative type of action: Simple Grant
Indicative type of implementation: ECCC
Type of beneficiaries: All entities

[30] See https://eur-lex.europa.eu/eli/dir/2022/2555
[31] See https://eur-lex.europa.eu/eli/reg/2019/881/oj
[32] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454
[33] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

2 Programme Support Actions

Programme support actions with indicative budget of EUR 6 million 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 WP 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

These activities are not subdelegated to other DGs.

3 Implementation

The programme counts with two main implementation modes: 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[34].

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 Appendix 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 ECCC, until the ECCC has the necessary capacity, 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.

Exclusion criteria

Applicants which are subject to EU administrative sanctions (i.e. exclusion or financial penalty decision)[35] might be excluded from participation. Specific exclusion criteria will be listed in the call for proposals.

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

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 Appendix 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[36] 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.
More information about these calls will be available on: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

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

[36] http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html

Table 4: Call timeline for topics in this Work Programme

Milestones	First set of calls of WP 2023-24	Second set of calls of WP 2023-24
Call Opening[37]	Q3-2023	Q2-2024
Deadline for submission[38]	Q1- 2024	Q3- 2024
Evaluation	Q1-2024	Q4 -2024
Information to applicants on the outcome of the call	Q1-2024	Q4-2024
Signature of contracts	Q2/Q3-2024	Q1/Q2-2025

Table 5: Indicative list of topics in the Second set of calls for proposals (grants and procurement) under this Work Programme (2024) with a common deadline

	Topics in the Work Programme
Security Operation Centres	Cross-Border SOCs Platforms
	Advanced Key Technologies for Cross-Border SOCs platforms
Cybersecurity Emergency Mechanism	Preparedness Support and Mutual Assistance
National Coordination Centres	National Coordination Centres
	Total Budget 111 M EUR

[38] The Director-General responsible for the call may delay this deadline by up to three months for individual topics or group of topics.

4 Appendices

4.1 Appendix 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 Appendix 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 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 grants 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 providing financial support to third parties. 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% of eligible costs for the consortium, co-financing of 50% of total eligible costs by the supported third party.

4.3 Appendix 3 - Implementation of Article 12(5) Regulation (EU) 2021/694

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[39] (including those established in the EU territory but controlled by a third country or by a third country legal entity). EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States.

The assessment of the foreign control is part of the eligibility criteria. For this purpose, 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.

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

In the particular case of section 1.1 (Security Operation Centres), legal entities established in eligible countries but judged to be controlled by a third country can participate in the calls for tenders, provided that they comply with the 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 section 1.1.

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

(a) control over the participant'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 participant complies with national security requirements applicable to procurement;

(c) the access by non-eligible third countries or by non-eligible third country entities to classified and non-classified sensitive information[40] relating to the action will be prevented;

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

(e) the results of the action shall remain within the contracting authority 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.

(f) For participant 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

[39] See article 12(5) of the Regulation (EU) 2021/694

[40] 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).

results, 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 procurement 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 documents.

PURCHASING FROM NON-EU ENTITIES UNDER JOINT PROCUREMENT

Specific security conditions set out for joint procurement must be objective, non-discriminatory and must be duly justified under Union law, including in accordance with the exceptions foreseen in the relevant international agreements. When deciding to set out security conditions the contracting authorities should take into account whether state of the art solutions are manufactured or developed by EU/EEA-based and EU/EEA-controlled entities. Where the contracting authorities open the market to suppliers that are not EU-controlled, the tendering documents shall set out that the goods or services (or components thereof) shall fulfil requirements that guarantee the protection of the essential security interests of the Union and the Member States and ensure the protection of classified information. The requirements shall be set out in the tendering documents and enable the participation of entities based in countries that are e.g. parties to a security agreement with Member States.

Goods or services provided by EU/EEA controlled entities may contain consumables and/or components manufactured outside of the EU/EEA provided that these consumables and/or components don’t raise any risk to the protection of the essential security interests of the Union and the Member States and ensure the protection of classified information.

4.4 Appendix 4 - Abbreviations and Acronyms

Abbreviation/ Acronym	Definition
AI	Artificial Intelligence
AI/ML	Artificial Intelligence and Machine Learning
CEF	The Connecting Europe Facility
CERT	The Computer Emergency Response Team
CRA	The Cyber Resilience Act
CSIRT	The Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
EC	The European Commission
ECCC	The European Cybersecurity Industrial, Technology and Research Competence Centre
EDIC	The European Digital Infrastructure Consortium
EDIH	European Digital Innovation Hub
EEA	The European Economic Area
EEA EFTA	The European Economic Area and the European Free Trade Association countries (Iceland, Liechtenstein, and Norway)
ERDF	The European Regional Development Fund
ERIC	The European Research Infrastructure Consortia
IoT	Internet of Things
ISACs	Information Sharing and Analysis Centers
MCPs	Multi-Country Projects
MS	Member States
NCCs	The Network of National Coordination Centres
NIS Directive	The Directive on Security of Network and Information Systems
NIS2 Directive	Revised NIS Directive
SIEM	Security Information and Event Management
SMEs	Small and Medium-sized Enterprises
SOC	Security Operation Centres
WP	Work Programme