EUROPEAN
COMMISSION

Brussels, 14.12.2023
C(2023) 8620 final

ANNEX 2

ANNEX

to the

Commission Implementing Decision

amending the Commission Implementing Decision C (2023) 1862 final on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024

ANNEX II
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 further develop the EU's 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]

However, the main DEP WP includes activities in the area of cybersecurity that will be implemented by the European Commission, namely those that aim to strengthen response to cyber threats and incidents across the EU through a mechanism that will support the efforts of the Member States. These activities are time-sensitive and are entrusted to ENISA which is better equipped to handle such tasks.

As the calls funded under this WP fall under Specific Objective 3: Cybersecurity and Trust of the Digital Europe Programme, they will be subject to the provisions of Article 12(5) of Regulation (EU) 2021/694 as detailed under each action. 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. European Economic Area-European Free Trade Association (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]

Actions under this work programme will also be in line with the Communication on the implementation of the 5G cybersecurity Toolbox[6].

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 Cybersecurity 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[7] to support preparedness (ex-ante), and response (ex-post) to

[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] Commission Communication on the Implementation of the 5G cybersecurity Toolbox, C(2023) 4049 final, 15 June 2023, https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

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

large-scale cybersecurity incidents via **Cybersecurity Emergency Mechanism**, in line with the proposed Cyber Solidarity Act[8]. This mechanism 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 Work Programme. The one on preparedness and mutual assistance is part of this Work Programme.

- Support cybersecurity capacity building at national and, where relevant, regional and local levels through **National Coordination Centres**, which will aim at fostering cross-border 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[9] 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)[10].

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 the action on Incident Response Support (Section 3 of the Main WP), the following actions are designed to reinforce EU's advanced cybersecurity capacities by addressing the cybersecurity skills shortage in Europe and by supporting investors with a focus on cybersecurity:

- 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

[8] See "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" COM(2023) 209.

[9] 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).

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

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.

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 (that is, entities not established in the EU, or established in the EU but not controlled by a Member State or national from of a Member State) 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, also considering the sensitive nature of specific objective 3 as indicated in this Regulation. 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, which will be distributed as follows:

- EUR 89 million for actions related to building capacities of Security Operation Centres,

- EUR 35 million for Artificial Intelligence and Advanced Key Technologies in Cybersecurity
- EUR 30 million for actions relating to the implementation of the proposed Cyber Resilience Act
- EUR 24 million for actions relation to the transition to Post-Quantum Cryptography
- EUR 70 million for actions in relations to the Cybersecurity Emergency Mechanism component on preparedness and mutual assistance, in line with the proposed Cyber Solidarity Act,
- EUR 3 million for coordination between the Cybersecurity Civilian and Defence Spheres,
- EUR 3 million for standardisation in the area of cybersecurity,
- EUR 50 million for support for implementation of EU legislation on cybersecurity and National Cybersecurity Strategies,
- EUR 65 million for actions to be carried out by National Coordination Centres,
- 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[11], 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 on Synergies between Horizon Europe and the ERDF programmes[12] 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.

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.

Funding from cohesion policy programmes and national budgets can fall under EU State aid rules when the beneficiaries are undertakings or supported activities are of an economic nature. In such cases, the funding must be compatible with EU State aid rules.

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, and further fund specific requirements may apply.

Table 2: Actions for which cumulative funding could be considered

Topics in the Work Programme	**DIGITAL Funding rate**

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

[12] 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

Security Operation Centres – National SOCs	50% for joint procurement and 50% for grants
Security Operation Centres – Cross Border SOCs	75% for joint procurement and 50% for grants
Cybersecurity Emergency Mechanism	50%
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"[13], 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[14]. 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 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 objectivesof 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.[15] The Multi-Country Project area of activities relevant for 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

[13] COM/2021/574 final

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

[15] 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.

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.

EU State aid rules apply to the public funding granted from Member State resources if that funding is for an economic activity or benefits this activity, and if all other cumulative conditions for the presence of State aid, set out in Article 107 (1) TFEU, are met.

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.

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 of calls for proposals (grants and procurement) under this Work Programme

Area	Topics in the Work Programme	Indicative budget (in million EUR)
Security Operation Centres	Call for Expression of Interest on National SOCs	20,8
	Call for Expression of Interest for Enlarging existing or Launching New Cross-Border SOC Platforms	22
	Joint Acquisition of Infrastructure, Tools and Services with Cross-Border Platforms	14,2
	Novel applications of AI and Other Enabling Technologies for Security Operation	30

	Centres	
	Strengthening the SOC ecosystem	2
Development and Deployment of Advanced Key Technologies	Development and Deployment of Advanced Key Technologies	35
Support for the Implementation of the proposed Cyber Resilience Act	Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations	22
	Tools for compliance with CRA requirements and obligations	8
Post-Quantum Cryptography	Deployment of Post Quantum Cryptography in systems in industrial sectors	22,25
	Standardisation and awareness of the European transition to post-quantum cryptography	1
	Roadmap for the transition of European public administrations to a post-quantum cryptography era	0,75
Cybersecurity Emergency Mechanism	Preparedness Support and Mutual Assistance, targeting larger industrial operations and installations	70
	Coordination Between the Cybersecurity Civilian and Defence Spheres	3
	Standardisation in the Area of Cybersecurity	3
Support to EU Legislation	Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2023)	30
	Support to EU cybersecurity legislation (2024)	20
National Coordination Centres	Deploying The Network of National Coordination Centres with Member States	65
Programme Support Actions		6
	Total	**375**

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 SOC platforms 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 of the relevant actors. 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 cross-border SOC platforms, for which a hosting and usage agreement will be

concluded, and 50% of the acquisition costs under joint procurement for National SOCs. Up to 50% of the running costs of National or Cross-Border SOC platforms may be covered by a complementing grant, provided necessary requirements are met. The remaining total cost of ownership of the National and Cross-Border SOC platforms shall be covered by the Participating States in the hosting consortium.

The actions under this topic are without prejudice to the proposed Cyber Solidarity Act[16].

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 Cyber Threat Intelligence (CTI), reviews and analyses. They provide a central operational capacity and support other SOCs at national level (e.g., by offering guidance or training, making available data or analysis of this data, coordinating joint detection and monitoring actions). They will play a central role at national level and can act as a hub within a context of SOCs in the different countries.

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 events, in close collaboration with relevant entities such as CSIRTs. They will also, where possible, benefit from information and feeds from other SOCs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis.

Scope

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

A key element is the translation of advanced AI/ML, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real

[16] See "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" COM(2023) 209

conditions in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms).

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

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

To achieve this aim, a call for expression of interest[17] will be launched to select entities in Member States that provide the necessary facilities to host and operate National SOCs. Applicants to the call for expressions of interest should describe the aims and objectives of the National SOC, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the National SOC, the services it will offer, the way they will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the National SOC, its services and its infrastructure.

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

- ***[Procurement] A Joint Procurement Action*** with the Member State where the national SOC is located: this will cover the procurement of the main equipment, tools and services needed to build up the National SOC
- ***[Building up and running the National SOC]*** A grant will also be available to cover, among others, the preparatory activities for setting up the National SOC, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National SOC, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

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

These actions aim at creating or strengthening national SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected

[17] 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.

against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

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 - workstream on Joint procurement with Member States
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[18]	2024
Indicative duration of the action	2-3 years
Implementation	ECCC
Type of beneficiaries	Public bodies acting as National SOCs, as identified by Member States
Security	The call for expression of interest comprising the two instruments, i.e., grants and Joint procurement is 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.

[18] For indicative timing see Table 4.

Type of action	Call for Expression of Interest - workstream on Simple Grants
Indicative budget	EUR 5,8 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[19]	2024
Indicative duration of the action	2-3 years
Implementation	ECCC
Type of beneficiaries	Successful applicants to the workstream on joint procurement
Security	The call for expression of interest comprising the two instruments, i.e., grants and joint procurement, is 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 Enlarging existing or Launching New Cross-Border SOC Platforms

Cross-border SOC platforms are collaborative platforms where National SOCs collaborate in a cross-border context. They should provide new additional capacity building upon and complementing existing SOCs and Computer Security Incident Response Teams (CSIRTs) and other relevant actors.

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 prevention capabilities in a trusted environment.

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

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

and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU.

Scope

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

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

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

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

A call for expression of interest[20] will be launched to select entities in Member States that provide the necessary facilities to host and operate Cross-Border SOC platforms for pooling data on cybersecurity threat between several Member States. Applicants to the call for expressions of interest should describe the aims and objectives of the Cross-Border SOC platform, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the Cross-Border SOC platform, the services it will offer, the way they will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the Cross-Border SOC platform, its services and its infrastructure.

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

[20] 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.

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

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

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

Deliverables

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

Type of action	Call for Expression of Interest – workstream on Joint procurement with Member States
Indicative budget	EUR 17 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]	2024
Indicative duration of the action	2-3 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	Call for Expression of Interest – workstream on Simple Grants
Indicative budget	EUR 5 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[22]	2024
Indicative duration of the action	2-3 years
Implementation	ECCC
Type of beneficiaries	Successful applicants to the workstream on joint procurement
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 Joint Acquisition of Infrastructure, Tools and Services with the Cross-Border SOC Platforms

[21] For indicative timing see Table 4.

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

Under the 2021-2022 work programme, a call for expression of interest[23] was launched that aimed to select entities in EU Member States and other eligible countries, willing to deploy and manage cross-border SOC platforms[24].

The selected consortia, ENSOC and ATHENA, will engage in joint procurement with the ECCC to purchase the necessary tools and infrastructures to establish the cross-border SOC platforms.

Objective

This action aims to support the joint procurement proposed by these two Cross-Border Platforms, selected through the call for Expression of Interest under the previous work programme. The expression of interest submitted at the time provide the detailed planning of the activities and tasks of each Cross-Border SOC platform, the services it will offer, the way they will operate and be operationalised, the duration of the activity and the main milestones and deliverables.

This will enable both platforms to achieve the objective of strengthening capacities to analyse, detect and prevent cyber threats and to support the production of high-quality intelligence on cyber threats, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention capabilities in a trusted environment.

Scope

The joint procurement proposed by the ENSOC and ATHENA consortia will cover main equipment, tools and services needed to build up the Cross-Border SOC platform. These joint procurements will be completed through this action. The selected consortia will engage in joint procurement with the ECCC to purchase the necessary tools and infrastructures to establish the cross-border SOC platforms. For each joint procurement, the EU will contribute up to 75% of the purchasing costs. The remaining procurement costs would be covered by Member States participating in each cross-border SOC platform.

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

These actions aim at creating or strengthening cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity

[23] 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.

[24] See https://cybersecurity-centre.europa.eu/system/files/2022-11/Call%20for%20Expression%20of%20Interest_Cross-border%20SOC%20platformsfinal.pdf

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

Deliverables

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

Type of action	Joint procurement with Member States
Indicative budget	EUR 14.2 million
Indicative call planning[25]	2024
Indicative duration of the action	2-3 years
Implementation	ECCC
Type of beneficiaries	Entities identified in CfEI under previous work programme
Security	Procurement 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.

[25] For indicative timing see Table 4.

1.1.4 Novel applications of AI and Other Enabling Technologies for Security Operation Centres

Objective

This topic addresses enabling technologies (such as AI) for SOCs, including National SOCs which provide a central operational capacity and support other SOCs at national level and play a central role as a hub within a context of SOCs, and also Cross-border SOC platforms where such technologies can strengthen capacities to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats.

These enabling technologies should allow more effective creation and analysis of Cyber Threat Intelligence (CTI), as well as faster and scalable processing of CTI and identification of patterns that allow for rapid detection and decision making.

Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity based on enabling technologies (such as AI), addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that indicate potential threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape.
- Creation of CTI based on novel threat detection capabilities.
- Enhancing speed of incident response through real-time monitoring of networks to identify security incidents and generating alerts or triggering automated responses.
- Mitigating malware threats by analysing code behaviour, network traffic, and file characteristics, reducing the window of opportunity for attackers to exploit malware.
- Identification and management of vulnerabilities.
- Recovery from incidents through self-healing capacities.
- Reducing the chances of attacks and pre-emptively identifying weaknesses through automated vulnerability scanning and penetration testing.
- Protecting sensitive data through the analysis of access patterns and detection of abnormal behaviour.
- Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymisation and de-identification. Tool and service providers are welcome to apply to this topic, also when in a consortium with National SOCs. Links with stakeholders in the area of High-Performance Computing should be made where appropriate, as well as activities to foster networking with such stakeholders.

Tool and service providers are welcome to apply to this topic, also when in a consortium with National SOCs. Links with stakeholders in the area of High-Performance Computing should be made

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

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

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

Deliverables

- Deployment of Artificial Intelligence and Advanced Key Technologies as enablers for SOCs
- Tools for creation, analysis and processing of CTI that allow for faster and more scalable SOC operations
- Original European CTI feeds or services

Type of action	Simple grant
Indicative Budget	EUR 30 million
Indicative call planning	Second set of calls
Indicative duration of the action	3 years
Implementation	ECCC
Type of beneficiaries	Technology providers, operators of SOCs, and other relevant stakeholders
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

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

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

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

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

Scope

Actions should address one or more of the following:

- Activities and technical frameworks that foster the collaboration and interconnection between Cross-Border SOC platforms and National SOCs, as well as fostering the link between National SOCs and other SOCs at national level.
- Actions that support the cooperation and coordination of Cross-Border SOC platforms, both between different Cross-Border SOC platforms, and with relation to national SOCs and other SOCs.
- Actions to foster links between public sector and industry, and stimulate mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities.
- Actions to foster links between SOCs and industrial stakeholders in artificial intelligence and in other enabling technologies, fostering the adoption of such technologies, including AI techniques and tools rand facilitating getting acquainted with existing state of the art tools (such as for example those developed in Action 1.1.4 of this work programme) and knowledge exchange.
- Actions to engage stakeholders from the HPC stakeholder community and practitioners of breakthrough AI technologies, to develop a blueprint for the requirements of AI models that necessitate access to large or smaller HPC facilities, and next steps to make this happen, as well as raising awareness of this in the wider SOC community.

These actions aim at creating or strengthening *national* and/or cross-border SOCs, which occupy a central role in ensuring the (cyber-)security *of* national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and

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

Deliverables

- Events, workshops, stakeholder consultations, architectural designs and white papers on technical coordination and interconnection support platforms.
- Stronger links between public sector and industry SOCs
- Technical frameworks to allow for information exchange between SOC platforms
- A blueprint for the use of HPC facilities for the benefit of SOCs

Type of action	Coordination and support action grant
Indicative budget	EUR 2 million
Indicative call planning	Fourth set of calls
Indicative duration of the action	3 years
Implementation	ECCC
Type of beneficiaries	National SOCs, Cross-Border SOC Platforms and other relevant stakeholders
Security	Call restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694

1.2 Development and Deployment of Advanced Key Technologies

Objective

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

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

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

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

Scope

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

- Real-time Monitoring and Incident Response: ensuring the swift identification and response to security incidents through continuous network monitoring, alert generation, and automated response mechanisms.
- Malware Defence and Analysis: mitigating malware threats by analysing code behaviour, scrutinizing network traffic, and assessing file characteristics, thereby reducing opportunities for attackers to exploit vulnerabilities.
- Proactive Vulnerability Management: identifying and addressing weaknesses proactively through automated vulnerability scanning and penetration testing to address potential threats before they can be exploited.
- Data Protection and Anomaly Detection: safeguarding sensitive data by scrutinizing access patterns and identifying abnormal behaviour to mitigate data breaches and protect critical information.
- Incident investigation to help uncover cause, scope and impact of security incidents or breaches that have occurred.
- Data Utilisation with Privacy: enabling organisations to harness data for analysis and insights while preserving data security and privacy through techniques such as anonymisation and de-identification.

By addressing such issues, the cybersecurity resilience of organisations should be enhanced, improving overall cybersecurity posture, encompassing various aspects such as threat detection, incident response, and vulnerability management.

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

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

This action aims at the deployment of key technologies in cybersecurity, in particular also in the context of securing national authorities, providers of critical infrastructures and essential services. As this involves the handling of cyber incidents, malware and management of vulnerabilities that could be exploited by malicious actors, the deployment of such technologies must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Deliverables

- Deployment of state-of-the-art technologies in the area of cybersecurity
- Tools for automated threat detection, monitoring of networks, data protection and incident response

Type of action	SME support action grant
Indicative Budget	EUR 35 million
Indicative call planning	Fourth set of calls
Indicative duration of the action	36 months
Type of beneficiaries	All entities
Implementation	ECCC
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

1.3 Support for the Implementation of the proposed Cyber Resilience Act

1.3.1 Strengthening cybersecurity capacities of European SMEs in line with Cyber Resilience Act requirements and obligations

Objective

The objective of this topic is to support European SMEs, with a focus on micro and small enterprises, to strengthen their cybersecurity capacities and to support the implementation of the proposed Regulation on the Cyber Resilience Act (CRA).

Scope

In synergy with other actions launched under this WP which will be developing compliance tools for the CRA, the action should distribute cascade financing grants to European SMEs, with a focus on micro and small enterprises, though remaining open to other stakeholders, to support achieving compliance with requirements and obligations stemming from the CRA.

Applicants are encouraged to identify categories of cascade financing recipients, including at least the following:

- Manufacturers of products with digital components, including software developers.
- Providers of tools and solutions that facilitate compliance with CRA obligations.
- Other well-justified categories in line with CRA (e.g., distributors, importers, open-source community).

For each identified stakeholder category, a dedicated set of activities should be devised taking into consideration the specific needs of target consumers, business users, and other relevant stakeholders.

The proposed project should include actions addressing the following:

- Awareness raising, dissemination and other stakeholder engagement actions with the focus on the cascade financing to European SMEs, with a focus on micro and small enterprises.
- Managing an open call process to distribute cascade funding, including impartial evaluation of proposals and monitoring the implementation of grants.
- Establish an openly available platform providing links to CRA-related resources that the proposed project itself would collect or develop or which would be available from external sources and supporting community building and upskilling. This includes for example a dedicated central repository website to allow easy finding of internal and external resources, step-by-step guidelines, compliance tools, training materials, free and open-source code implementations, and other relevant resources to achieve CRA compliance. This should include, amongst others, tools procured for this purpose under this work programme.
- In close coordination with the EU Cybersecurity Skills Academy, perform trainings and upskilling of stakeholders to achieve CRA compliance, i.e. organise workshops, training sessions, and events, draft guidelines, supporting actions to facilitate interaction among European SMEs, including drafting reports or other material discussing the implementation of CRA compliance requirements and promoting awareness, including by contributing to relevant deliverables of standardisation bodies e.g. through a sectoral perspective and informed by the needs of companies on the ground.
- Facilitate and share CRA compliance best-practices and use-cases.
- Contribute to standardisation efforts, as appropriate, considering the activities of European and international standardisation that are directly relevant to the CRA implementation.

Third parties receiving grants should, in particular:

- Engage in testing, detecting and addressing vulnerabilities, producing documentation, carrying out conformity assessment and implementing other measures necessary to comply with the CRA.

- Participate in workshops, training sessions, and events that facilitate interaction among European SMEs, with a focus on micro and small enterprises, to discuss and implement CRA compliance.

- Contribute to the proposed project's efforts in collecting the needs and perspectives of SMEs towards CRA-related standardisation deliverables.

Priority should be given to solutions available to use free of charge or free and open-source software (FOSS) solutions both when setting up the openly available platform and when distributing cascading finance grants.

These activities should be carried out in close coordination, and where possible collaboration, with the European Cybersecurity Competence Centre (ECCC), the Network of National Coordination Centres (NCCs), the European Digital Innovation Hubs (EDIHs) network, other relevant European and National cybersecurity entities, and other projects of this work programme.

The operational involvement of NCCs in implementing and running such actions is strongly recommended.

Indicatively one proposal is expected to be financed via this topic. Proposed projects should foresee at least 75% of the budget to be distributed for cascade financing grants.

This action includes the creation of a central platform that serves as a reference point, and hence will enable interactions between providers of essential services and critical infrastructures, as well as other actors, regarding their cybersecurity measures and possible vulnerabilities. Also third parties receiving funding will engage in solutions for testing, detecting and addressing vulnerabilities. As such information could be exploited by malicious actors, the central entity handling such must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Deliverables:

- Financial support for SMEs and other stakeholders for CRA compliance.
- Openly available platform with CRA-related resources (such as guidelines and supporting documents), providing supporting community building and upskilling
- Workshops, events, networking and exchange of experience of stakeholders
- Contributions to CRA standardisation

Type of action	Grant for Support to Third Parties

Indicative Budget	EUR 22 million
Indicative call planning	Second set of calls
Indicative duration of the action	36 Months
Implementation	ECCC
Type of beneficiaries	All stakeholders
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

1.3.2 Tools for compliance with CRA requirements and obligations

Objective

The objective of this topic is to support the implementation of the proposed Cyber Resilience Act (CRA) through tools that support, and where possible automate, internal compliance procedures, including testing and specification drafting with focus towards European SMEs, in particular micro and small enterprises.

Scope

This action aims at the design and development of tools to facilitate, and where possible automate, CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements and documentation obligations.

CRA compliance solutions are foreseen based on technical specifications, training modules, and other relevant material. Tools for penetration testing, testing facilities and other cybersecurity practices, aligning with CRA requirements, are also in the scope.

Tools should be tailored towards needs of European SMEs, with a focus on micro and small enterprises, though also usable by broader stakeholder categories, such as:

- Manufacturers of relevant product categories falling within the scope of the CRA, including software developers.
- Others, such as distributors, importers, open-source community, etc.

CRA compliance tools should be made widely available on fair and reasonable terms and also take into consideration the specific needs of different stakeholders such as the behaviour of consumers, business users, and other relevant factors.

Priority should be given to solutions available to use free of charge or free and open-source software (FOSS) solutions.

These activities should be carried out in close coordination and, where possible collaboration, with the Network of National Coordination Centres (NCCs), the European Digital Innovation Hubs (EDIHs)

network, the EU Cybersecurity Skills Academy, other relevant European and National cybersecurity entities, and other projects of this work programme.

This action aims at the creation of tools that, amongst others, do penetration testing or document technical specifications with relation to cybersecurity, including for entities that are providers of essential services and critical infrastructures. As such tools and information could be exploited by malicious actors, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Deliverables:

- Tools to simplify and automate CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements.
- Tools to simplify and automate CRA compliance documentation obligations.

Type of action	SME support action grants
Indicative Budget	EUR 8 million
Indicative call planning	Second set of calls
Indicative duration of the action	12-18 months
Implementation	ECCC
Type of beneficiaries	Technology providers
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

1.4 Post Quantum Cryptography

1.4.1 Deployment of Post-Quantum Cryptography (PQC) systems in industrial sectors

The stability of Europe's economic activities and the integrity of its single market heavily rely on the seamless functioning of underlying digital infrastructures, services, and data integrity. However, the emergence of quantum computers poses a potential long-term security threat to these digital frameworks, which is especially crucial for critical sectors like energy, transport, health, and finance.

Post-Quantum Cryptography (PQC) is crucial to overcome this emerging threat. Ensuring data confidentiality, secure communication, and the enduring integrity of stored information necessitates the seamless integration of PQC into foundational infrastructures across various sectors. By proactively adopting PQC, organisations can foster secure collaboration, protect critical assets, and ensure operational continuity in the era of quantum computing, thereby strengthening long-term security and safeguarding sensitive information.

Objective

The objective is to enable the adoption of PQC in industrial sectors like automotive, automation, finance, control systems or energy. The overarching aim is to seamlessly integrate PQC systems, equipment, components, protocols, and network technologies into existing digital security and communication networks.

Scope

Proposals should focus on the integration of a standardised PQC protocol into the digital security and communication networks in the automotive, automation, finance, or energy sector, while taking into account specific needs of the sector, such as necessary keys strength and keys management. Proposals should cover the development or adaptation of the required software/hardware and the validation of the solution in a large-scale demonstrator. This includes creating an inventory of assets requiring protection with a quantified level of risk, a migration plan[26] for both the migrating entities and their suppliers and customers, taking into account data protection policies, contributing to the development of standards and certification. Successful consortia are expected to raise awareness on the need to transition to PQC and share their experience and best practice.

This action aims at the creation of a technology that will be used to protect the cybersecurity of critical industrial assets with a new paradigm that is set to be a game changer in encryption. The control of such tools is of utmost importance for governments and industry alike, as they could be exploited by malicious actors. As such, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- PQC system validation and PQC technology ready for wide-spread deployment in given industrial sectors
- Long-term protection of critical assets, long-term information security and operational continuity in the advent of quantum computers

[26] See for example https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

- Migration checklists and plans for PQC in sectors where this has not yet taken place.

Type of action	Simple grant
Indicative Budget	EUR 22.25 million
Indicative call planning	Second set of calls
Indicative duration of the action	Up to 36 months
Implementation	ECCC
Type of beneficiaries	Industry actors and related stakeholders
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

1.4.2 Standardisation and awareness of the European transition to post-quantum cryptography

The objective of post-quantum cryptography (PQC) is to construct cryptographic systems that remain secure against both classical and quantum computers, while seamlessly integrating with existing communication protocols and networks. Europe has taken a pioneering role in PQC research, developing cryptographic suites and packages. These innovations include secure key-encapsulation mechanisms and secure digital signature algorithms, that are contributing to translating academic research in the field into practical technologies and industrial applications.

Objective

Proposals should aim to strengthen Europe's efforts on the transition to PQC by supporting European and international standardisation activities, delivering a comprehensive European PQC industrial migration roadmap and raise awareness regarding PQC endeavours. This should be achieved in particular through the following strategic actions:

- Organisation of events, workshops, stakeholder consultations, and production of white papers to fostering the development of harmonised standards on PQC.
- Support for participation of relevant European experts in European and international standardisation fora relating to PQC.
- Community-Based PQC Migration Roadmap: Foster a collaborative process involving research and industry stakeholders to formulate a robust European PQC migration roadmap, which can be the basis for sector-specific roadmaps.
- Widespread Dissemination of PQC Outcomes: Promote broad awareness and understanding of European PQC achievements through extensive dissemination efforts spanning various platforms, including social media. This includes outreach events and structured dialogues with the general public, exploring ethical and societal dimensions of PQC, especially in terms of privacy, security, public trust, and acceptance.

- Research Dissemination Services: Provide specialised dissemination services targeting relevant communities, such as European cybersecurity providers and users, effectively sharing research insights.
- Identifying Training and Infrastructure Needs: Identify crucial requirements for training, education, and infrastructure to advance PQC development.

Scope

Proposals are expected to engage in concrete standardisation efforts within both European and international standardisation forums, where PQC will play a pivotal role in the near future and where progress in standardisation will augment existing cybersecurity capabilities and create a competitive edge upon Europe. Also, in alignment with projects resulting from the topic "Transition to Quantum-Resistant Cryptography" (call HORIZON-CL3-2022-CS-01-03) and the topic Deployment of Post-Quantum Cryptography (PQC) systems in industrial sectors (in this work programme), the proposals will incorporate practical strategies to coordinate and synergise European research and innovation endeavours with PQC standardisation initiatives.

To this end, proposals should establish a proactive presence and take on leadership roles in orchestrating and shaping international standards and regulations for PQC. This can either be in existing standardisation activities and bodies or, where relevant, by contributing to creating new standardisation activities in existing groups and/or creation of new groups.

Proposals should cultivate a cohesive European PQC community, fostering collaboration among academic and industrial stakeholders, and engage in a structured dialogue on various fora. This will entail harmonising activities across European, national, and regional programs and projects, and pave the way for synergetic innovation efforts in PQC to help unlock use-cases for practical cybersecurity applications in Europe.

Proposals should bring together key stakeholders across the entire PQC value chain. This holistic approach should encompass researchers, standardisation experts and representatives from industry sectors. A comprehensive outline should be provided in the proposal, detailing the stakeholders to be engaged and the methodologies to efficiently coordinate their efforts at the European level in order to achieve impactful outcomes that effectively promote European interests in PQC standardisation.

Furthermore, the proposals will strive to establish constructive dialogues with international PQC programmes and promote international cooperation activities. Emphasis should be placed on collaborative exchanges between key international participants, including the EU and countries such as the USA, exploiting complementary strengths and challenges and fostering mutually beneficial outcomes in standardisation efforts.

This action aims at supporting stakeholders dealing with technologies that will be used to protect the cybersecurity of critical industrial assets with a new paradigm that is set to be a game changer in encryption. The control of such tools is of utmost importance for governments and industry alike, as they could be exploited by malicious actors. As such, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.

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

Outcomes and deliverables

- Contributions to European and international standards and regulations in PQC
- Workshops, white papers and other activities to support synergies between different sectors transition to PQC
- A European PQC migration roadmap, which can be the basis for sector-specific roadmaps
- Actions supporting the European PQC community
- Development of standards for hybrid cryptographic systems (pre- and postquantum encryption systems) for encryption, key encapsulation mechanisms, digital signatures, etc. and for the PQC integration in the existing digital infrastructure .
- Support for participation of relevant European experts in European and international cross-topical standardisation bodies in order to integrate PQC whenever new cryptographic standards are developed or existing ones are updated especially for critical sectors like energy, transport, health, and finance.

Type of action	Coordination and support action grant
Indicative Budget	EUR 1 million
Indicative call planning	Second set of calls
Indicative duration of the action	Up to 36 months
Implementation	ECCC
Type of beneficiaries	Stakeholders in the field of cryptography, PQC and/or standardisation
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694

1.4.3 Roadmap for the transition of European public administrations to a post-quantum cryptography era

Public administrations handle and exchange vast amounts of sensitive information related to national security, intelligence and defence. Additionally, they store personal data of citizens, including for example healthcare data. It is crucial to protect such information in the long term and maintaining resilience against evolving threats. Since implementing PQC will be a complex and time-consuming process, exchange and coordination at national and European level in this area is needed to ensure PQC is rapidly and widely adopted by public administrations.

Objective

Proposals should foresee a leading role for national security agencies in developing a roadmap for the transition of public administrations to post-quantum cryptography PQC. This should take into account an inventory of systems to be replaced, the timeframe, and technical and legal aspects of the migration to PQC in public administrations. It should be achieved in particular through the following strategic actions:

- Foster a collaborative process involving stakeholders from national security agencies and other public administrations to discuss priorities, technical challenges, legal obstacles and other issues relating to the transition to PQC.
- Promote awareness among public administrations of the need to make the transition to PQC.
- Identify crucial requirements and establish a coordinated roadmap for the transition of European public administrations to PQC.

Scope

Proposals should bring together national security agencies, relevant public administrations and related stakeholders including experts in the area of PQC. Activities should be foreseen to engage stakeholders to efficiently coordinate their efforts at national and European level in order to achieve impactful outcomes leading to the adoption of PQC in European public administrations.

The roadmap should identify what encryption systems need to be replaced, what algorithms should be adopted, priorities for defending against quantum attacks across the spectrum of public administrations, and legal and technical aspects of the transition to PQC. It should foster collaborations and exchange of best practice.

This action aims at the transition of public administration towards a new paradigm that is set to be a game changer in encryption, which directly involves national security as it relates to information that must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- Roadmap for the transition of European public administration for PQC
- Workshops, white papers and other activities to support synergies between national security agencies and public administrations.
- Collaborations between public administrations regarding the transition to PQC.

Type of action	Coordination and support action grant
Indicative Budget	EUR 0.75 million

Indicative call planning	Second set of calls
Indicative duration of the action	Up to 36 months
Implementation	ECCC
Type of beneficiaries	National Security Agencies and related stakeholders
Security	Call restricted on the basis of article 12(5) of the Regulation (EU) 2021/694

1.5 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[27], it was announced that as part of the proposal for an EU Cyber Solidarity Act[28], the Commission is preparing actions to strengthen preparedness and response actions across the EU. This work programme will support the proposed EU Cyber Solidarity Act 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 to the above 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** and one on **preparedness and mutual assistance**.

The activities relating to Incident Response Support will be implemented by the European Commission and are therefore in the Main DIGITAL WP. These activities are time-sensitive and are entrusted to ENISA which is better equipped to handle such tasks.

[27] Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence (JOIN(2022)49)

[28] See "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" COM(2023) 209

This WP contains the action on preparedness and mutual assistance, which is described below. This action is without prejudice to the proposed Cyber Solidarity Act.

1.5.1 Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

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, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Scope

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

Support for testing for potential vulnerabilities:

- Development of **penetration testing** scenarios. The proposed scenarios may cover Networks, Applications, Virtualisation solutions, Cloud solutions, Industrial Control systems, and IoT.
- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.
- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant**.**
- Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities.

Support for threat assessment and risk assessment:

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

Risk monitoring service:

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

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

This action aims at the creation of platforms that serve as a reference point and provide services such as penetration testing and threat assessments for providers of essential services and critical infrastructures, as well as other actors. This involves data and operational measure regarding cybersecurity, including penetration tests and exploitable vulnerabilities. Such information could be exploited by malicious actors, and thus it must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Deliverables:

- preparedness support services
- threat assessment and risk assessment services
- risk monitoring services

Type of action	Grant for Financial Support
Indicative budget	EUR 70 million
Indicative call planning	First and fourth 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

1.6 Coordination between the Cybersecurity Civilian and Defence Spheres

Objective

The objective is to enhance exchange and coordination between the cybersecurity civilian 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

1.7 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)[29], in 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 proposed 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

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

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 spill overs and subsequent costs to society to mitigate the risks associated with non-secure products.

Deliverables

- Organisation 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 standardisation 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

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

1.8.1 Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2023)

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]

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

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

and the proposed Cyber Resilience Act[32], and the Directive on attacks against information systems (Directive 2013/40)[33]. 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 the following 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).
- 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.

[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

- 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.
- Organisation 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
Implementation	ECCC

Type of beneficiaries	All entities
Security	Call restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694

1.8.2 Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

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)[34], the Cybersecurity Act[35], and the Directive on attacks against information systems (Directive 2013/40)[36]. It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous Digital Work Programme.

In addition, this action also aims at supporting the implementation of the proposed Cyber Resilience Act[37] (CRA) by market surveillance authorities/notifying authorities/national accreditation bodies, by increasing their capacities to ensure effective implementation of the CRA.

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

- Development of trust and confidence between Member States.
- Supporting market surveillance authorities/notifying authorities/national accreditation bodies to implement the CRA.
- Effective operational cooperation of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services including public authorities.
- Better security and notification processes and means for Essential and Important Entities in the EU, including cross-border (automated) incident notification systems.
- Better reporting of cyber-attacks to law enforcement authorities in line with the Directive on attacks against information systems.
- Improved security of network and information systems in the EU.
- More alignment of Member States' implementations of NIS2 (Directive (EU) 2022/2555).
- Support cybersecurity certification in line with the Cybersecurity Act.

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

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

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

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

Scope

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

- Implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents.
- Increasing capacity for market surveillance authorities/notifying authorities/national accreditation bodies in view of tasks as provided by the CRA.
- Collaboration, communication, awareness-raising activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).
- Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.
- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.
- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.
- Enable businesses across all sectors and consumers to use products with digital elements securely.
- Support to Cybersecurity certification, including support to national cybersecurity certification authorities and other relevant stakeholders, such as SMEs. This includes activities such as threat-led penetration testing, acquiring certification testbeds, sharing best practices, implementing innovative evaluation methods for specific ICT products or components.

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

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

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

This action seeks to support the European cybersecurity posture by creating a European ecosystem of companies and organisations that will support the implementation of EU cybersecurity legislation that will contribute to strengthening the European capacities in protecting the cyberspace. The results from the work carried out in the projects funded under this action may include implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents involving cybersecurity of providers of essential services and critical infrastructures, as well as other actors. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Deliverables

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organisation of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions and cooperation for further advanced of cybersecurity certification.
- Effective supervision and enforcement of the CRA by the market surveillance authorities and adequate capabilities of notifying authorities and national accreditation bodies for the implementation of the CRA.

Type of action	Simple grant
Indicative budget	EUR 20 million
Indicative call planning	Fourth set of calls
Indicative duration of the action	36 months
Implementation	ECCC
Type of beneficiaries	All entities
Security	Call restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694

1.9 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 (NCCs) – 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[38], Cybersecurity Act[39]).

The objective is to support the operation of the NCCs and to enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities.

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 EECCC in achieving its objectives and missions;
- providing expertise and actively contributing to the strategic tasks of the ECCC, 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 ECCC, 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;
- 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 ECCC, 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);

[38] Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15–69).

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

- promoting and disseminating the relevant outcomes of the work of the Network and the ECCC 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 NCC;
- advocating and promoting involvement by relevant entities in the activities arising from the ECCC, 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.

The aim is also to provide essential support in the domain of cybersecurity in the form of financial support to third parties. The funding should foremost facilitate the adoption and widespread use of state-of-the-art cybersecurity solutions. This should equip organisations with the latest and most effective tools and strategies available for cybersecurity, fortifying their overall cybersecurity capabilities, and helping them to become more resilient and better prepared to face the evolving challenges posed by cyber threats in the digital age.

Such support should be in synergy with other actions undertaken by NCCs, such as their role as contact point, promotion of participation in cross-border projects and actions, establishing synergies with other activities, and fostering links with the ECCC and other relevant national and European actions such as the Digital Innovation Hubs.

This topic targets exclusively National Coordination Centres which have been recognised 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.

Indicatively 50% of the grant will be distributed via financial support to third parties.

These actions aim at the operation of National Coordination Centres, which occupy a central role in the cybersecurity landscape as foreseen in Regulation (EU) 2021/887. Due to the synergetic role, they play with regards 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, they must be able to handle sensitive information, and be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Outcomes and deliverables

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

- Uptake of cybersecurity solutions
- Strengthened cybersecurity capacities of stakeholders
- Synergetic activities that strengthen the role of NCCs

Type of action	Simple Grant
Indicative Budget	EUR 65 million
Indicative call planning	Two calls or two cut-off dates aligned with third set and fourth set of calls
Indicative duration of the action	48 months
Indicative budget per grant (EU contribution)	EUR 2 million, with a maximum of EUR 5 million per NCC
Implementation	ECCC
Type of beneficiaries	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
Security	Call restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694

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 (including presidency events)
- publications
- communication
- studies
- other support measures, e.g. support to the Cyber Security Atlas

These activities are not sub delegated 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[40].

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 strategy choices will be subject to pre-approval by the European Commission Information Technology and Cybersecurity Board.

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

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

Applicants which are subject to EU administrative sanctions (i.e. exclusion or financial penalty decision)[41] 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 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[42] 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.

---

[41] See Article 136 of EU Financial Regulation 2018/1046.

[42] 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 4: Call timeline for topics in this Work Programme

Milestones	First set of calls of WP 2023-24	Second set of calls 2023-24	Third set of calls 2023-24	Fourth set of calls of WP 2023-24
Call Opening	Q2-2023	Q4-2023	Q1-2024	Q3-2024
Deadline for submission[43]	Q3- 2023	Q2-2024	Q2- 2024	Q4-2024
Evaluation	Q4-2023	Q2-2024	Q2 -2024	Q1-2025
Information to applicants on the outcome of the call	Q4-2023	Q3-2024	Q3-2024	Q1-2025
Signature of contracts	Q2 /Q3-2024	Q4-2024	Q1/Q2-2025	Q3/Q4-2025

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

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 of the Digital Europe Programme can exclude the participation of legal entities controlled by a third country [1] (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), exceptionally, when in order to fulfil the objectives of the European Cyber Shield, it is necessary, for duly justified reasons, to procure the provision of subscription services for information aiming to enhance cybersecurity situational awareness, the procuring authority may allow legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States to use as subcontractors, suppliers established in or controlled by third countries, subject to strict security conditions, in order to ensure sufficient diversity and geographical coverage of the information in the subscription services procured.

Where the contracting authorities allow the use of subcontractors who are suppliers that are not EU-controlled, the tendering documents shall set out that the 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. Such security conditions 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.

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