ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme (DIGITAL)

Call for proposals

Deploying Strategic Cyber Capabilities Across Europe

(DIGITAL-ECCC-2025-DEPLOY-CYBER-09)

Version 1.0
23 October 2025

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	23.10.2025	• Initial version.	

CALL FOR PROPOSALS

Contents

0. Introduction

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

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

- Regulation 2024/2509 (EU Financial Regulation)[1]
- the basic act (Digital Europe Regulation 2021/694[2]).

The call is launched in accordance with the 2025-2027 Work Programme[3] and will be managed by the European Cybersecurity Competence Centre (ECCC).

⚠ Please note that this call is subject to possible amendments of the 2025 - 2027 Work Programme. In case there are substantial changes, the call may be modified. All updates will be reflected in the call document.

The call covers the following **topics**:

- **DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI- Cybersecure tools, technologies and services relying on AI**
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE– Uptake of innovative cybersecurity solutions for SMEs**
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP– Coordinated preparedness testing and other preparedness actions**
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS– Regional Cable Hubs**

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

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

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

- the Call document outlines the:
  - background, objectives, scope, outcomes and deliverables, KPIs to measure outcomes and deliverables, targeted stakeholders, type of action and funding rate and specific topic conditions (sections 1 and 2)
  - timetable and available budget (sections 3 and 4)
  - admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)

[1] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) ('EU Financial Regulation') (OJ L, 2024/2509, 26.9.2024).

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

[3] Adopted by the GB of ECCC concerning the adoption of the work programme for 2025-2027 amendment.

  - criteria for financial and operational capacity and exclusion (section 7)
  - evaluation and award procedure (section 8)
  - award criteria (section 9)
  - legal and financial set-up of the Grant Agreements (section 10)
  - how to submit an application (section 11).
- the Online Manual outlines the:
  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
  - recommendations for the preparation of the application.
- the AGA — Annotated Grant Agreement contains:
  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc)*.

You are also encouraged to visit the EU Funding & Tenders Portal to consult the list of projects funded previously.

1. Background

Digital transformation is accelerating at an unprecedented pace, reshaping the core of our economies and societies. From AI-enhanced services to quantum computing, these technologies are redefining how we interact, produce, and safeguard information. Yet, this evolution also brings a new generation of threats - more complex, stealthy, and globally disruptive. Recent geopolitical tensions, coupled with increasingly sophisticated cyberattacks, highlight the pressing need for Europe to fortify its digital sovereignty and resilience.

To address these challenges, the EU continues to invest strategically in its cybersecurity capabilities through the Digital Europe Programme. The third Work Programme (2025–2027) developed by the European Cybersecurity Competence Centre (ECCC), outlines a comprehensive framework to secure the Union's digital future in alignment with the EU Cybersecurity Strategy, the Cyber Solidarity Act, and the ECCC Strategic Agenda.

The 2025 call 9 focuses on six critical areas of cybersecurity deployment:

• **Cybersecure AI Tools and Services**: Artificial intelligence is transforming cybersecurity—both as a tool and a target. This action supports the development and deployment of AI-powered cybersecurity solutions to enhance threat detection, incident response, and threat intelligence, while ensuring that AI systems themselves are secure, trustworthy, and compliant with EU legislation such as the AI Act and GDPR.

• **Cybersecurity Support for SMEs through AI**: European SMEs are often under-resourced and vulnerable to cyberattacks. This action provides AI-enabled, user-friendly cybersecurity tools tailored to their needs, helping them manage cyber risks, report incidents, and strengthen their overall cyber resilience.

• **Uptake of Innovative Cybersecurity Solutions for SMEs**: Despite a wealth of innovation, the uptake of advanced cybersecurity tools among SMEs remains limited.

This action fosters the deployment of proven solutions by facilitating access, providing financial incentives, and supporting integration into business operations.

• **Coordinated Preparedness Testing and Actions**: The EU's cybersecurity readiness must be rigorously tested. This call supports stress testing, simulations, and other preparedness actions, including cross-border and cross-sector to strengthen the ability of critical infrastructure operators to prevent and respond to cyber incidents.

• **EU Action Plan on Cable Hubs**: Submarine cable systems are vital to Europe's digital and economic security. This action will reinforce the cybersecurity of cable hubs—physical and digital entry points—ensuring they are robust against espionage, sabotage, and system failures.

These initiatives are subject to Article 12(5) of the Digital Europe Programme Regulation, ensuring that entities involved meet EU security requirements.

Together, these actions aim to create a more secure, sovereign, and resilient digital Europe. They will support the deployment of advanced technologies while safeguarding European values, democracy, and the competitiveness of the internal market in an increasingly contested digital domain.

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

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI - Cybersecure tools, technologies and services relying on AI

Objectives

This topic addresses AI-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies and private entities from the NIS 2 directive, NCCs[4], etc. They play a key role in providing central operational capacity to European cybersecurity ecosystems. They may also provide primary input data for AI/ML-based cybersecurity tools and solutions, which can strengthen such authorities' capacity to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats. In particular, the adoption of generative AI[5] could be a challenge and an opportunity for cybersecurity[6] processes and applications.

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

The security of AI itself, especially for the systems in the learning phase, also needs to be addressed, including the misuse of AI by malicious actors. This includes

[4] If applicable and in line with individual national strategies.

[5] Cybersecurity in the age of generative AI, September 2023, available at: https://www.mckinsey.com/featured-insights/themes/cybersecurity-in-the-age-of-generative-ai.

[6] The Need For AI-Powered Cybersecurity to Tackle AI-Driven Cyberattacks, April 2024, available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered-cybersecurity-to-tackle-ai-driven-cyberattacks.

carrying out risk assessments and mitigation of cybersecurity risks inherent to AI technologies, implementing supply chain security, etc., and complying with the AI Act, intellectual property legislation and the GDPR.

In addition to being secure, the AI technologies being developed should perform well, and be robust and trustworthy. In particular, having trustworthy AI solutions will help in the deployment phase, where social acceptance is essential.

Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity[7], based on AI technologies[8], addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. These activities must also comply with intellectual property rights (IPR) and the GDPR, depending on the type of information handled. The AI solutions proposed should also be cybersecure.

Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that can potentially indicate emerging threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape, including in ICT or in Operational Technology infrastructures using open technologies.
- 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 of vulnerabilities and support for management considering multiple sources of information.
- Cybersecure tools and solutions that provide risk-reduction in the crossover between AI, IoT and smart grids or other manufacturing chains.
- Support for 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 business 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.
- Tools and solutions that provide product security or cybersecurity by design/default in line with CRA requirements.
- Tool and service providers are welcome to apply for this topic, also when in a consortium with Cyber Hubs. 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. In well justified cases,

[7] Multilayer Framework for Good Cybersecurity Practices for AI, ENISA, June 2023, available at: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai.

[8] Cybersecurity of AI and Standardisation, ENISA, March 2023, available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation.

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 licensing to National and/or Cross-Border Cyber Hubs platforms, CSIRTs, competent authorities, and other relevant authorities under favourable market conditions.
- These actions aim at providing AI-powered cybersecurity capabilities for National and/or Cross-Border Cyber Hubs and for national authorities encompassing Cyber Hubs, CSIRTs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. These entities are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of their crucial operative role in ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, Cyber Hubs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.
- Tools to protect and secure AI solutions in line with the EU legislative framework and considering integration of requirements for robustness, performance, trust and balanced AI autonomy.
- Contribute to the cybersecurity certification of AI-driven cybersecurity solutions and systems. The primary objective of cybersecurity certification for AI systems within the EU is twofold: to mitigate cybersecurity risks inherent in AI technologies and to demonstrate compliance with the EU's comprehensive legislative framework, including the AI Act. By establishing a standardised, transparent, and rigorous certification process, the EU seeks to foster trust in AI technologies among users, developers, and regulators alike.

Expected Outcomes

- Deployment of Artificial Intelligence and various AI-powered technologies as enablers for Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Novel cybersecurity tools based on AI that have been developed, tested and validated in relevant conditions and made available to Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Enhanced information sharing and collaboration amongst National and Cross-Border Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others relevant stakeholders, supported by CTI produced by AI-powered tools.
- Tools for automation of cybersecurity processes such as the creation, analysis and processing of CTI, to enhance operations of the Cyber Hubs.
- Original European CTI feeds or services.
- Ensure that the most advanced and innovative secure AI solutions are developed and implemented for NIS sectors.
- Secure AI solutions and tools, complying with EU legislation. Promote the mitigation of risks associated with the misuse of AI by malicious actors, with a focus on AI ethics and secure deployment.
- Contribution to the standardisation and certification of cybersecure, trustworthy AI technologies.

KPIs to measure outcomes and deliverables

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

When applicable, baseline and target values must be provided.

- Number of entities benefitting from project activities.
- Number of AI-powered cybersecurity technologies and capabilities provided for National and/or Cross-Border Cyber Hubs and for national authorities encompassing Cyber Hubs and CSIRTs.
- Number of AI services and enabling technologies deployed for rapid detection of cybersecurity incidents and more effective decision making.
- Number of tools for automated threat detection and incident response.
- Number of cybersecure tools and solutions that provide risk-reduction in the crossover between AI, IoT and smart grids or other manufacturing chains.
- Number of original Cyber Threat Information (CTI) feeds created and deployed in operational environment.
- Number of tools and solutions that provide product security or cybersecurity by design/default in line with CRA requirements.
- Number of tools to protect and secure AI solutions in line with the EU legislative framework.

Targeted stakeholders

Cyber Hubs operators, technology providers, research and academia, cybersecurity entities, NIS 2 Directive entities and other relevant stakeholders supporting the deployment of cyber-secure AI solutions, end-users.

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

Type of action and funding rate

Simple Grants — 50% funding rate

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

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment*(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE– Uptake of innovative cybersecurity solutions for SMEs

The action aims at improving industrial and market readiness for the cybersecurity requirements for SMEs as specified in relevant EU cybersecurity legislation, for instance, as set in the Cyber Resilience Act ensuring more secure hardware and software products.

Objectives

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

- Availability of innovative tools and services that support SMEs in complying with the EU cybersecurity legislation.
- Availability of innovative tools and services that support SMEs in reporting incidents and in assisting with recovery if possible, and in exchanging with competent authorities (i.e. cooperation with Cyber Hubs, CSIRTs (including in relation to the CSIRT Network) and/or ISACs, for e.g. highly critical and other critical sectors entities).
- Improved security and notification processes and means in the EU.
- Improved security of network and information systems in the EU.
- Industrial and market readiness for the proposed Cyber Resilience Act.
- Support for Cybersecurity certification in line with the Cybersecurity Act.
- Support for supply chain partners in standardised self-assessments and certifications. Helping downstream supply chain partners in a step-by-step approach to increase cyber resilience.
- Overcome the challenge of finding the technical skills required to deal with a complex technology landscape that relies heavily on extensive configurations and capabilities.
- Cyber toolkit as a service to support for SMEs[9] managing cyber risks, defining, and implementing their cybersecurity strategy, including several functions dedicated to risk assessment, vulnerabilities and threats detection, etc.
- Support and incident response capabilities to SMEs.

Scope

The action will focus on supporting at least one of the following priorities listed below, in the next section.

Expected Outcomes

The development of a cyber toolkit as a service to support SMEs managing cyber risks, defining, and implementing their cybersecurity strategy. The toolkit could include at least one of the following:

- Interfaces that will connect to existing SaaS applications such as HR, invoice and financial management, CRM and accounting systems, etc., which are often used by SMEs for increasing their cybersecurity.
- A functionality that enables the mapping and maintenance of an SME's digital assets and possible vulnerabilities by interfacing with other SaaS applications that manage an asset inventory and data repositories.

[9] Cybersecurity guide for SMEs - 12 steps to securing your business, ENISA, 2021, available at: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes.

- A function that supports the assessment and management of an SME's cybersecurity risks and of supply chain risk management. This function should perform a risk assessment, provide recommendations for risk mitigation, and identify options.
- An interface to existing tools that support the analysis and assessment of the extent of an SME's cyber risk based on information gathered from digital infrastructure scanning and data provided by authorised users.
- A function that issues alerts on vulnerabilities and threats based on the information collected by the risk management function.
- A function that connects SMEs to a CSIRT or a Cyber Hub to report an incident and assist with recovery if possible.
- A mapping and one-stop window/portal to existing tools and solutions targeting cybersecurity support to SMEs.
- Tools supporting detection, prevention and response in Operational Technology infrastructures using open standards or technologies.

Support and incident response capabilities to SMEs:

- Non-commercial cybersecurity hotline with a standardised framework and guidelines for response times, escalation procedures, and the scope of assistance provided.
- A fully operational, multilingual helpline that provides timely and accurate cybersecurity assistance to SMEs, leading to reduced successful cyber scams and improved digital hygiene.
- A National Cyber Response Platform for first cyber responders to exchange their experiences, share relevant news and engage discussions regarding challenges and emerging cyber threats complementary to existing cyber crisis management structures.
- Specialised training modules for first (public and private) responders' services targeting different sectors such as healthcare, finance, energy, and transportation.

Support tools and platforms:

- Control Centre and Panel on Incident Reporting and dispatching of incident responders.
- SME user interface for Incident reporting associated with the cyber toolkit. Users can report an incident, get instructions on how to react and obtain information on how to receive support for the response. An AI assistant connected to a Control Centre could also be included.
- Interfaces with the National Authorities and Cross-Border Platforms (CBPs) for incident notification and information sharing.

KPIs to measure outcomes and deliverables

Applicants shall provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice. When applicable, baseline and target values must be provided.

- Number of entities benefitting from project activities.
- Number of cybersecurity new technologies deployed in operational environments.
- Number of innovative tools and services that support SMEs in reporting incidents, assisting with recovery and in exchanging with competent authorities.

- Number of cybersecurity tools and services that support SMEs in managing cyber risks, defining, and implementing their cybersecurity strategy, including risk assessment, vulnerabilities and threats detection.

Targeted stakeholders

This topic targets in particular SMEs but other applicants, such as private and public entities implementing NIS 2 Directive, Cyber Resilience Act, research and academia and end-users can be also considered.

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

Type of action and funding rate

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

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

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP–Coordinated preparedness testing (other preparedness actions covered only in 2026 and 2027)

This topic covers actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism, namely coordinated preparedness testing of entities operating in sectors of high criticality across the Union, specifically the health sector, and in particular hospitals, and the digital infrastructure sector, including electronic communication sector, and in particular fixed networks and submarine cable infrastructure.

Objectives

These actions aim 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 critical industrial installations and infrastructures, by assisting Member States in their efforts to improve their preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving coordinated preparedness testing of entities operating in sectors of high criticality across the Union (including penetration testing and threat assessment) considering ICT as well as Operational Technology/Industrial Control Systems.

Scope

The provision of preparedness support services shall include the activities listed below, for entities in the sector or sub-sector as identified by the Commission in accordance with the Cyber Solidarity Act, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 and specified in the call for proposal document for each of the calls under this topic.

For 2025 the selected sectors are the health and in particular hospitals and the digital infrastructure sector, including electronic communications and in particular fixed networks and submarine cable infrastructures.

Applications may cover more than one sector. Selected proposals, at call level, will have to cover all selected sectors and sub-sectors.

The scope includes 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 and important entities operating critical infrastructure for potential vulnerabilities (vulnerability scanning).

- Support for the deployment of digital tools and infrastructures enabling 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 highly critical sectors (Annex I to Directive (EU) 2022/2555) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.

- Evaluation, including security audits, and/or testing of cybersecurity capabilities of MS entities and MS sectors (including capabilities to prevent, detect and respond to incidents and **stress test of the entire sectors**), evaluation and compliance activities aimed at increasing maturity, e.g. on the basis of established maturity models and/or relevant evaluation and compliance schemes.

- Evaluation, including security audits, and/or testing of cybersecurity capabilities of entities in scope (including for the evaluation and management of risks concerning the supply chain).

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

Support for **threat assessment and risk assessment, such as**:

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

The support will target the competent authorities in the Member States, which play a central role in the implementation of the NIS 2 Directive, such as Computer Security Incident Response Teams (CSIRTs) and National Cybersecurity Authorities.

The Cyber Solidarity Act provides as well that the coordinated preparedness testing should be conducted using common risk scenarios and methodologies that should be developed by the NIS Cooperation Group in cooperation with the Commission, EEAS, ENISA and, within the remit of its mandate, EU-CyCLONe.

Risk scenarios are a key component for engaging in coordinated preparedness testing activities. Building on risks and vulnerabilities previously identified in sectorial, national and/or EU level risk assessments, risk scenarios support and guide coordinated preparedness testing by providing "what-if" situations where the effect of risks materialising is measured.

Risk scenario development typically incorporates features such as severity, likelihood and escalation levels over a baseline. Aggravation levels stages are key to realistically assessing resilience under increasing pressure. A gradual aggravation of severity can be delivered either by scaling the impact of a single scenario or layering either multiple sub-scenarios or attack vectors together for each variation.

The proposed risk scenarios for this call are in 3 different critical sectors:

- For health sector – risk scenarios affecting hospitals;
- For digital infrastructure sector – risk scenarios affecting submarine cable infrastructures;
- For digital infrastructure sector – risk scenarios affecting fixed networks.

Risk scenarios are detailed in chapter 4 of the annex 3. They adopt a multi-layer approach by using a baseline scenario and two additional scenarios (with aggravation levels), each compounding on the previous one.

Annex 3 proposes as well as a methodology that could be used in the coordinated preparedness testing in the three sub-sectors. The methodology could differ between the three sub-sectors.

Each applicant may choose among the proposed risk scenarios what they would use for the national action (included in the proposal). However, the proposal should include at least **one baseline scenario** (which is the first one for each three sub-sectors in annex 3). Applicants may adapt the scenarios and include elements based on their national context, on top of the general EU-wide risk scenarios. Member State may choose to include higher intensity scenarios proposed in annex 3. For the national action, applicants are encouraged to explore systemic risks by covering also the supply chain dimension and interdependencies.

Applicants may also consider expanding the risk scenarios to reflect the cumulative effects of multiple, possibly smaller, incidents. These may include incidents affecting individual organisations as well as supply chain disruptions occurring in parallel with the main scenario. Furthermore, applicants are encouraged to balance the focus across different types of incidents, including system failures, human error, malicious acts, and natural phenomena.

Results of the coordinated preparedness testing could be integrated in the remediation plan of the tested entity and shall be sent to the Member State authority to review the

results of the action. These lessons learned should be shared, in an anonymised and aggregated form, with the Commission. A follow-up discussion could take place in the relevant workstreams of the NIS Cooperation Group.

Coordinated preparedness testing has 3 main phases:

A. **Systemic risk analysis phase**

In this phase a more high-level systemic risk assessment:

- Identify key stakeholders
- Decide on scope
- Refine risk scenarios

B. **Testing phase**

In this phase the testing takes place. This can take the form of:

- Vulnerability Scanning
- Security Audits
- Penetration Testing
- Exercises
- (Cyber Resilience) Stress Tests

C. **Gap analysis phase**

In this phase the coordinated preparedness test results are converted to actionable recommendations:

- Identify gaps
- Recommendations
- Action plan

Expected Outcomes

- Enhanced cooperation, preparedness and cybersecurity resilience in the EU; preparedness support services

- Services such as: threat assessment, risk assessment services, security audits, scanning for vulnerabilities, exercises, stress tests of the entire or part of the sectors.

KPIs to measure outcomes and deliverables

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

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

- number of penetration tests provided
- number of essential and important entities supported
- number of threat assessments / risk scenario analyses carried out
- number of risk monitoring services provided
- number of potential users covered per test/exercise
- number and nature of vulnerabilities discovered
- number of cross-border actions/exercises

Targeted stakeholders

Public bodies acting as cybersecurity competent authorities or CSIRTs. Public bodies subject to the NIS 2 Directive, CRA, CSA, CSoA, DORA etc.

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

Type of action and funding rate

Simple Grants — 50% funding rate

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

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS– Regional Cable Hubs

As part of the EU Action Plan on Cable Security, it was announced that the Commission, together with voluntary Member States, will work on Cable Integrated Surveillance Mechanisms per sea basin ('Regional Cable Hubs') to enhance the detection capacity against threats to undersea cables as they are critical infrastructure.

Taking into account the fact that these cables are covered by the scope of NIS2 Directive that follows an all-hazards approach, it is crucial to protect their physical environment from events such as malicious acts, including cuts as integral part of the cable cybersecurity measures.

Objectives

The objective is to support the progressive establishment of Regional Cable hubs, one per sea basins of the EU, whose role will be to concretely enhance threats detection and operational security around these strategic infrastructures.

This action is therefore aimed at supporting the set-up of processes, tools and services for detection and analysis of emerging threats, to establish a near real time situational

awareness to protect the undersea cables. It includes the capacity to aggregate data and security information from all available sources (including established systems such as the Integrated Maritime System, or CISE, or National Cyber Hubs) and analyse them in an automated way. The action will support also the establishment of a reporting incident function and a procedure for information sharing between relevant national authorities.

Additionally, structured partnership with private sector to enhance the voluntary information sharing for cable security as well as the potential and progressive integration of the relevant defence dimension capacities – in a dual use approach – could be considered in the action.

Should the participating Member States so decide, the regional cable hubs could coordinate the deployment and activation of modular repair equipment across a sea basin.Finally, the scope could also cover the acquisition of additional capacities, equipment, tools, instruments or services useful for the enhancing the resilience and security of undersea cables.

Expected outcomes

The Regional cable hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection, supporting the development of an operational capacities to ensure the security and resilience of undersea cables.

The hubs should act as a central point allowing for broader pooling of data and information relevant for the security environment of the cables, enabling the dissemination of threat information and incident detection on a regional scale and among a diverse set of national actors as designated by each Member States (e.g. National Hubs, CSIRTs.)

The Hubs should allow a rapid exchange of information, even if classified among participating authorities in a given hub. To that end, the participating authorities shall set procedural arrangements on cooperation and information sharing.

Furthermore, regional cable hubs could also benefit from additional solutions for the surveillance and protection of submarine cables, and the detection of malicious activities. For instance, situational awareness performed through the collection and analysis of in-situ, sea-based sensor data as well as relevant satellite imagery or undersea drones capacities.

The Hubs could make use of existing systems which were not developed necessarily for Cable Security, such as the Integrated Maritime Systems, the Common Information Sharing Environment (CISE), the EU Copernicus Space Programme, and the Maritime Surveillance System. (MARSUR).

The Hubs should also integrate direct cooperation with private entities, especially cable operators to increase access – in a highly secured framework - to information on ongoing and future threats and voluntary incident reporting.

The Hubs should progressively also integrate the defence dimension, as any defence capacities is likely to increase the situational awareness as well as the capacity to respond fast in case of incident against these strategic critical infrastructures. To that end, Member States can integrate in the operations of the Hubs their defence capacities (e.g. navy or surveillance system) and operational command while building on international partnerships.

To support the above activities of a Regional Cable Hub, a grant will be available to cover, among others, the preparatory activities for setting up the Regional Cable Hub, its interaction and cooperation between its members and with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Regional Cable Hub. The grant could also be used to cover the acquisition of the infrastructures, tools and services needed to build-up the Regional Cable Hub but also to equip it with the necessary capacities to enhance the security and resilience of undersea cables, such as detection capacities.

These actions aim at creating or strengthening Regional Cable Hubs, which occupy a central role in ensuring the Security and resilience of strategic and critical infrastructures, providers of essential services such as global connectivity and power supply. As previously noted, Regional Cable Hubs will have a crucial operative role in ensuring the security of undersea cables in the Union and will handle sensitive information.

Pursuant to Article 12 of Regulation (EU) 2021/694, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme.

KPIs to measure outcomes and deliverables

- Number of processes, tools and services to protect the undersea cables.
- Number of solutions for the surveillance and protection of submarine cables and the detection of malicious activities.
- Number of active collaborations to increase access to information on cyber threats and voluntary incident reporting.
- Cyberthreat intelligence and situational awareness services developed.
- Number of tools for automated threat detection and incident response.

Targeted stakeholders

Any public authority, agency or entity in charge in Member States of Cable Security, Maritime security, resilience or protection of critical infrastructures, as well as other relevant stakeholders specialized in maritime surveillance technologies, cybersecurity and threat detection, data aggregation and AI-driven analysis and critical infrastructure resilience.

The involvement of the largest number of eligible entities pertinent for the sea-basin is strongly encouraged.

Type of action and funding rate

Simple Grants — 70% funding rate

The funding rate of this action is exceptionally increased due to the geopolitical importance of the activities funded under this topic.

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

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6)
- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

3. Available budget

The estimated available call budget is **EUR 50 000 000**.

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

Topic	Topic budget
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI	**EUR 15.000.000**
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE	**EUR 15.000.000**
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP	**EUR 10.000.000**
DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS	**EUR 10.000.000**

The availability of the call budget still depends on the final adoption of the 2025-2027 Work Programme amendment.

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

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	28 October 2025
Deadline for submission:	31 March 2026 – 17:00:00 CET (Brussels)
Evaluation:	April - May 2026
Information on evaluation results:	June - July 2026
GA signature:	November 2026

5. Admissibility and documents

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

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the *Topic page in the Search Funding & Tenders section).*

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

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

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project *(to be filled in directly online)*
- Application Form Part B — contains the technical description of the project *(template to be downloaded from the Portal Submission System, completed, assembled and re-uploaded)*
- **mandatory annexes and supporting documents** *(templates to be downloaded from the Portal Submission System, completed, assembled and re-uploaded)*:
  - detailed budget table/calculator: not applicable
  - CVs of core project team: not applicable
  - activity reports of last year: not applicable
  - list of previous projects: not applicable
  - ownership control declarations (including for associated partners and subcontractors): applicable

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that all participants comply with the conditions for receiving EU funding *(especially eligibility, financial and operational capacity, exclusion, etc)*. Before signing the grant, each beneficiary and affiliated entity will have

to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable**, **accessible and printable** (please check carefully the layout of the documents uploaded).

Proposals are limited to maximum **70 pages** (Part B) for topics:

- DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI- Cybersecure tools, technologies and services relying on AI
- DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE– Uptake of innovative cybersecurity solutions for SMEs
- DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP– Coordinated preparedness testing and other preparedness actions
- DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS– Regional Cable Hubs

Evaluators will not consider any additional pages.

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

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

6. Eligibility

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

Eligible participants (eligible countries)

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

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

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

Other entities may participate in other consortium roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc *(see section 13)*.

Please note however that all topics of this call are subject to restrictions due to security reasons, therefore entities must not be directly or indirectly controlled from a country

that is not an eligible country**. All entities[10] will have to fill in and submit a declaration on ownership and control.**

Moreover:

– participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is limited to entities established in and controlled from eligible countries

– project activities (included subcontracted work) must take place in eligible countries (see section geographic location below and section 10)

– the Grant Agreement may provide for IPR restrictions (see section 10).

For more information, see Annex 2.

Specific cases and definitions

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

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

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons[11].

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

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[12]. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

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

EU restrictive measures — Special rules apply for entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[13]. Such entities are not eligible to

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

[11] See Article 200(2)(c) EU Financial Regulation 2024/2509.

[12] For the definitions, see Articles 190(2) and 200(2)(c) EU Financial Regulation 2024/2509.

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

participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

EU conditionality measures — Special rules apply for entities subject to measures adopted on the basis of EU Regulation 2020/2092[14]. Such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties, etc). Currently such measures are in place for, Hungarian public interest trusts established under the Hungarian Act IX of 2021 or any entity they maintain (see Council Implementing Decision (EU) 2022/2506, as of 16 December 2022).

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

Consortium composition

For the Topic **DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS– Regional Cable Hubs** a minimum of 2 independent applicants (beneficiaries; not affiliated entities) from 2 different eligible countries.

Eligible activities

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

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

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

Projects must comply with EU policy interests and priorities *(such as environment, social, security, industrial and trade policy, etc)*. Projects must also respect EU values and European Commission policy regarding reputational matters (*e.g. activities involving capacity building, policy support, awareness raising, communication, dissemination, etc*).

Financial support to third parties is not allowed in any topic under this call.

Geographic location (target countries)

Due to restrictions due to security:

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

[14] Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 325, 20.12.2022, p. 94).

Ethics

Projects must comply with:

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

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

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

Security

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

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

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
    - created or accessed only on premises with facility security clearance (FSC) from the competent national security authority (NSA), in accordance with the national rules
    - handled only in a secured area accredited by the competent NSA
    - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)

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

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

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

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

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

7. Financial and operational capacity and exclusion

Financial capacity

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

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

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

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

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

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

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities *(see below, section 10)*
- prefinancing paid in instalments
- (one or more) prefinancing guarantees *(see below, section 10)*

or

- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

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

Operational capacity

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

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

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

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

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project
- description of the consortium participants

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

Exclusion

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

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct[17] (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation,

[16] See Articles 138 and 143 of EU Financial Regulation 2024/2509.

[17] 'Professional misconduct' includes, in particular, the following: violation of ethical standards of the profession; wrongful conduct with impact on professional credibility; breach of generally accepted professional ethical standards; false declarations/misrepresentation of information; participation in a cartel or other agreement distorting competition; violation of IPR; attempting to influence decision-making processes by taking advantage, through misrepresentation, of a conflict of interests, or to obtain confidential information from public authorities to gain an advantage; incitement to discrimination, hatred or violence or similar activities contrary to the EU values where negatively affecting or risking to affect the performance of a legal commitment.

decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of EU Regulation 2988/95 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- intentionally and without proper justification resisted[18] an investigation, check or audit carried out by an EU authorising officer (or their representative or auditor), OLAF, the EPPO, or the European Court of Auditors.

Applicants will also be rejected if it turns out that[19]:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

8. Evaluation and award procedure

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

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

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

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

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

[18] 'Resisting an investigation, check or audit' means carrying out actions with the goal or effect of preventing, hindering or delaying the conduct of any of the activities needed to perform the investigation, check or audit, such as refusing to grant the necessary access to its premises or any other areas used for business purposes, concealing or refusing to disclose information or providing false information.

[19] See Article 143 EU Financial Regulation 2024/2509.

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

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

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

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

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

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

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

9. Award criteria

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

1. Relevance

- Alignment with the objectives and activities as described in section 2
- Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*
- Extent to which the project can overcome financial obstacles such as the lack of market finance*

2. Implementation

- Maturity of the project

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

3. Impact

- Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements
- Extent to which the project will strengthen competitiveness and bring important benefits for society
- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects ***.**

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

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

Maximum points: 15 points.

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

Overall threshold: 10 points.

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

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

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

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

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

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement *(Data Sheet, point 1)*. Normally the starting date will be after grant signature. A retroactive starting

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

Project duration:

- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI, DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE, and DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS the indicative duration of the action is 36 months, other durations are not excluded.
- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP the indicative duration of the action is 24 months, other durations are not excluded.

In very exceptional cases extensions are possible, through an amendment, if duly justified and agreed by the Granting Authority.

Milestones and deliverables

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

The following deliverables will be mandatory for all projects:

- additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project;
- additional deliverables (yearly) on achievement of relevant KPIs and project outputs.

Form of grant, funding rate and maximum grant amount

The grant parameters *(maximum grant amount, funding rate, total eligible costs, etc)* will be fixed in the Grant Agreement *(Data Sheet, point 3 and art 5)*.

Project budget (requested grant amount):

- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI: indicatively between 3 and 5 million EUR per project but other amounts, if duly justified, are not excluded.
- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE: approximatively 3 million EUR per project but other amounts, if duly justified, are not excluded.
- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP: approximatively 1.5 million EUR per project but other amounts, if duly justified, are not excluded.
- for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS: approximatively 3 million EUR per project but other amounts if duly justified, are not excluded.

The grant awarded may be lower than the amount requested.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted*

costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement *(see art 6 and Annex 2 and 2a)*.

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

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

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

Budget categories and cost eligibility rules

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

Budget categories for this call:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties (not applicable)
  - D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices)[20]: Yes
  - SME owner/natural person unit cost[21]: Yes

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

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

- travel and subsistence unit costs[22]: No (only actual costs)
- travel costs: eligible only in EU and EEA countries
- equipment costs:
  - depreciation + full cost for listed equipment (for all topics)
- other cost categories:
  - costs for financial support to third parties: not allowed
  - internally invoiced goods and services (unit cost according to usual cost accounting practices)[23]: Yes
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).
- VAT: non-deductible/non-refundable VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
  - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
  - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
  - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
  - restrictions due to security:
    - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
    - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible
  - other ineligible costs: No.

Reporting and payment arrangements

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

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

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

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

There will be one or more **interim payments** (with cost reporting through the use of resources report).

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

All payments will be made to the coordinator.

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

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

Prefinancing guarantees

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

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

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

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

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

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

Certificates

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

Liability regime for recoveries

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

For beneficiaries, it is one of the following:

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

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

or

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

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

Provisions concerning the project implementation

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

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

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

- background and list of background: Yes
- protection of results: Yes
- exploitation of results: Yes
- rights of use on results: Yes
- access to results for policy purposes: Yes
- access to results in case of a public emergency: Yes
- access rights to ensure continuity and interoperability obligations: No
- special IPR obligations linked to restrictions due to security:
  - exploitation in eligible countries: Yes
  - limitations to transfers and licensing: Yes

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

- communication and dissemination plan: Yes
- dissemination of results: Yes
- additional dissemination obligations: Yes
- additional communication activities: Yes
- special logo: both EU and European Cybersecurity Competence Centre logo

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

- specific rules for PAC Grants for Procurement: No
- specific rules for Grants for Financial Support: No

- specific rules for blending operations: No
- special obligations linked to restrictions due to security:
  - implementation in case of restrictions due to security or EU strategic autonomy: Yes

Other specificities

Consortium agreement: Yes in case of multi-beneficiary proposal.

Non-compliance and breach of contract

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

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

11. How to submit an application

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

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

a) **create a user account and register your organisation**

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

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

b) **submit the proposal**

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

Submit your proposal in 3 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and upload it as a PDF file
- Annexes (*see section 5*). Upload them as PDF file (single or multiple depending on the slots). Excel upload is sometimes possible, depending on the file type.

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

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

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

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the IT Helpdesk webform, explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

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

12. Help

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

- Online Manual
- Topic Q&A on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- Portal FAQ (for general questions).

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

Contact

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

Non-IT related questions should be sent to the ECCC Applicants Direct Contact Centre (ADCC), only after consultation of the National Coordination Centre, at the following email address: applicants@eccc.europa.eu

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

13. Important

IMPORTANT

- **Don't wait until the end —** Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions *(e.g. congestion, etc)* will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System —** By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the Portal Terms & Conditions.
- **Registration —** Before submitting the application, all beneficiaries, affiliated entities and associated partners must be registered in the Participant Register. The participant identification code (PIC) (one per participant) is mandatory for the Application Form.
- **Consortium roles** When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

  The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting, in very exceptional cases, may go beyond 30% of the total eligible costs and must be duly justified in the application.
- **Coordinator —** In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any). If affiliated entities participate in your project, please do not forget to provide documents demonstrating their affiliation link to your organisation as part of your application.
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget** Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully *(e.g. own contributions, income generated by the action, financial contributions from third parties, etc)*. You may be requested to lower your estimated costs, if they are ineligible (including excessive).

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

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

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

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

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

  Organisations may participate in several proposals.

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

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

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

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

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

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

  This includes:

  - beneficiary names
  - beneficiary addresses
  - the purpose for which the grant was awarded
  - the maximum amount awarded.

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

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

Annex 1

Digital Europe types of action

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

Simple Grants

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

Funding rate: 50% Simple Grants — The funding rate may be exceptionally changed in very specific cases and always in accordance with the approved Work Programme.

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

SME Support Actions

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

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

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

Coordination and Support Actions (CSAs)

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

Funding rate: 100%

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

Grants for Procurement

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

Funding rate: 50%

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

PAC Grants for Procurement

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

Funding rate: 50%

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

Grants for Financial Support

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

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

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

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

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

Lump Sum Grants

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

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

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

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

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

Funding rate: no funding for FPA

SGAs

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

Funding rate: 50%

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

Annex 2

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

Security restrictions Article 12(5) and (6)

If indicated in the Digital Europe Work Programme, and if justified for security reasons, topics can exclude the participation of legal entities *established* in a third country or DEP associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including DEP associated countries)[24].

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

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

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

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

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

⚠ EEA countries (and participants from EEA countries) are exempted from these restrictions (and additional requirements) because EEA countries benefit from a status equivalent to the Member States.

In order to determine the ownership and control status, participants[25] will be required to fill in and submit an ownership control declaration* as part of the proposal (and later on be requested to submit supporting documents) *(see Guidance on participation in EU restricted calls with ownership and control restrictions*)*.

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

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

Thus:

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

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

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

Strategic autonomy restrictions Article 18(4)

If indicated in the Digital Europe Work Programme, calls can limit the participation to entities *established* in the EU, and/or entities established in third countries associated to the programme for EU strategic autonomy reasons[26].

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

For more information, *see* *Guidance on participation in EU restricted calls with ownership and control restrictions**.

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

Annex 3

Coordinated Preparedness Testing under the Cyber Solidarity Act

1. Introduction and framework

The Cyber Solidarity Act that entered into force on 4th February 2025, as part of the preparedness actions, provides for the Coordinated Preparedness Testing of entities operating in sectors of high criticality (Annex I of NIS 2 Directive). The Coordinated preparedness testing shall be provided mainly in the form of grants managed by the European Cybersecurity Competence Centre.

According to the Cyber Solidarity Act, the Commission should identify the sectors for the coordinated preparedness testing, after consulting the NIS Cooperation Group, EU CyCLONe and ENISA. Such consultation took place at the beginning of this year, where the Commission proposed two sectors to be considered for the first call for proposals in 2025, namely: the health sector and in particular hospitals and the digital infrastructure sector, including electronic communication sector (where a subsector could be chosen for the coordinated preparedness testing).

The Cyber Solidarity Act provides as well that the coordinated preparedness testing should be conducted using common risk scenarios and methodologies that should be developed by the NIS Cooperation Group in cooperation with the Commission, EEAS, ENISA and, within the remit of its mandate, EU-CyCLONe.

The draft DEP Work Programme 2025-2027 aligns with the general principles of the Cyber Solidarity Act and provides that beneficiaries for this action could be public bodies acting as cybersecurity competent authorities or CSIRTs, public bodies subject to the NIS 2 Directive, CRA, CSA, CSoA, DORA etc. The activities funded under the calls could contain the support for testing for potential threats, vulnerabilities, and dependencies, including penetration testing, testing of physical and cybersecurity capabilities of Member States entities and sectors, including risk assessment and stress test of the entire sectors.

This paper proposes to work on risk scenarios in 3 different critical sectors:

- For health sector – risk scenarios affecting hospitals;
- For digital infrastructure sector – risk scenarios affecting submarine cable infrastructures;
- For digital infrastructure sector – risk scenarios affecting fixed networks.

This paper proposes as well to work on the methodology (elements of methodology) that could be proposed to be based on the coordinated preparedness testing in the three subsectors. The methodology could differ between the three subsectors. For the

development of methodology, ENISA's work on Good Practices Guide on Cyber Resilience Stress Testing is accounted for[27].

The Nevers risk assessment of 2024 already developed risk scenarios for the digital infrastructure sector, notably the communications infrastructures and networks. With its strategic recommendation number 8, the Nevers assessment specifically emphasises the need to extend physical stress testing to digital infrastructure.

2. Work arrangement and approach

Sectoral workstreams (Health and 5G/Telecom) have worked on risk scenarios affecting hospitals and fixed networks, respectively. The risk scenario(s) on submarine cable infrastructures was prepared in the Submarine Cable Infrastructure Expert Group, which based its methodology (in addition to the reference points mentioned above) on the 2025 cybersecurity risk assessment methodology by the NIS Cooperation Group and the stress test methodology developed for the energy sector in the context of the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure from 2022[28]. After discussions in sectoral workstreams and groups, the WS on risk assessment and supply chains reviewed all risk scenarios and the methodology(ies) and is sending the document to the NIS CG plenary.

3. Coordinated preparedness testing methodology and implementation approach

Each participating Member State may choose among the proposed risk scenarios (see chapter 4) what they would use for the national action (included in the proposal). However, the proposal should include at least **one common scenario**, which was decided to be the baseline scenario (which is the first one for each three subsectors). Member States may adapt the scenarios and include elements based on their national context, on top of the general EU-wide risk scenarios. Member stay may choose to include higher intensity scenarios proposed in this paper. For the national action, Member States are encouraged to explore systemic risks by covering also the supply chain dimension and interdependencies. For instance, the impact of an incident can increase when an organisation is (1) dependent on the affected service, and (2) lacks alternative services. This risk on societal level is particularly critical when multiple organisations rely on the same service (such as a specific type of software), since a disruption can have widespread, simultaneous affect.

Member States may also consider expanding the risk scenarios to reflect the cumulative effects of multiple, possibly smaller, incidents. These may include incidents affecting individual organisations as well as supply chain disruptions occurring in parallel with the main scenario. Furthermore, Member States are encouraged to balance the focus across different types of incidents, including system failures, human error, malicious acts, and natural phenomena.

[27] ENISA Good Practices Guide on Cyber Resilience Stress Testing

[28] COUNCIL RECOMMENDATION on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure

Results of the coordinated preparedness testing should be integrated in the remediation plan of the tested entity and should be sent to the Member State authority to review the results of the action. These lessons learned should be shared, in an anonymised and aggregated form, with the Commission. A follow-up discussion could take place in the relevant workstreams of the NIS Cooperation Group.

Coordinated preparedness testing has 3 main phases:

B. **Systemic risk analysis phase**

In this phase a more high-level systemic risk assessment:

- Identify key stakeholders
- Decide on scope
- Refine risk scenarios

C. **Testing phase**

In this phase the testing takes place. This can take the form of:

- Vulnerability Scanning
- Security Audits
- Penetration Testing
- Exercises
- (Cyber Resilience) Stress Tests

D. **Gap analysis phase**

In this phase the coordinated preparedness test results are converted to actionable recommendations:

- Identify gaps
- Recommendations
- Action plan

4. Risk Scenarios

Risk scenarios are a key component for engaging in coordinated preparedness testing activities. Building on risks and vulnerabilities previously identified in sectorial, national and/or EU level risk assessments, risk scenarios support and guide coordinated preparedness testing by providing "what-if" situations where the effect of risks materializing is measured.

Risk scenario development typically incorporates features such as severity/impact (how disruptive the scenario is expected to be), plausibility/likelihood (how likely the scenario is possible or not, including extreme events like a "black swan" or a "one-hundred-year event"), and aggravation/escalation levels over a baseline. Aggravation levels or scenario escalation stages are key to realistically assessing resilience under increasing pressure. A gradual aggravation of severity can be delivered either by scaling the impact of a single scenario or layering either multiple sub-scenarios or attack vectors together for each variation.

The following risk scenarios adopt a multi-layer approach by using a baseline scenario and two additional scenarios (with aggravation levels), each compounding on the previous one. For each risk scenario, we provide a short description of the scenario together with its primary impacts.

a. Hospitals

1. Unpatched website vulnerabilities, website developed and managed by a 3rd party supplier, ransomware infection, critical patient care not affected, some regular/planned care needs to be rescheduled. Critical care not affected, but some impact on non-critical care.

2. Phishing, ransomware, spreading into IT environment of laboratories, in some hospitals there is spill-over to OT/medical devices, lateral movement, extortion attempts of the hospital and individual patients. Some impact on critical care, serious disruption of non-critical care

3. Pandemic/flu-spike context, DDoS attack, ransomware attack, ransomware spreading to several hospitals, affecting also IT environment and also medical devices, the online EHR system is unavailable, which disrupts both non-critical and critical care, patients have to be moved to other hospitals (cross-border dimension). Severe impact on both critical care and non-critical care, patients being moved to other hospitals, also across the border

Risk scenario 1 – Low stress level (mandatory baseline scenario)

Unpatched website vulnerabilities, website developed and managed by a 3rd party supplier, ransomware infection, critical patient care not affected, some regular/planned care needs to be rescheduled. Critical care not affected, but some impact on standard/planned care.

Scenario 1: Ransomware attack on one hospital, affects several hospitals in a region Website vulnerability, third party supplier, drive-by-download, ransomware outbreak, hospital	
Scenario steps	**Impact**
• A threat actor exploits an unpatched vulnerability in a hospital's website, which is developed and managed by a 3rd party, and is used for keeping track of regional stocks of supplies and medicines. • The attackers compromise the webserver and upload ransomware, for a subsequent drive-by download attack, infecting the PCs of end-users visiting the website, which are different staff members at various hospitals across the region, are infected with ransomware. • When the PCs of these hospital staff are infected with ransomware, the ransomware automatically starts to propagate across their IT networks infecting other PCs in the IT networks of these hospitals.	• Backoffice staff in several hospitals can no longer do their work, leading to backlogs in administrative tasks, and problems with appointment scheduling and re-scheduling. • Critical care continues, but there is some disruption of patient care, due to loss of access to administrative data and appointment scheduling systems. • Patient care is affected because stocks of medical supplies cannot be accessed/managed and certain supplies are no longer available.

Risk scenario 2 – Medium stress level

Phishing, ransomware in the IT environment of a laboratory, spreading to other hospitals, and in some hospitals, there is spill-over to OT/medical devices, against a backdrop of extortion attempts of the hospital and some individual patients (some other types of impact). Some impact on critical care, serious disruption of standard/planned care.

Scenario 2: Phishing attack on a medical lab, leads to ransomware outbreak across various hospitals in the region, affecting also some medical devices. Phishing, ransomware, laboratory, IT and medical device environment, hospital, extortion	
Scenario steps	**Impact**
• Phishing attack successfully targets employees at a laboratory, compromising several PCs. • Attackers subsequently exploit an unpatched vulnerability to compromise a website, where lab results are published, inserting ransomware on that website to infect website visitors. • Ransomware spreads to several hospitals, infecting IT environments and in some cases also disabling several legacy medical devices. • The attackers try to extort the hospitals affected and a large number of individual patients affected by the data breach.	• Laboratory, used by several hospitals in the region, is offline for days and stops most of its business processes. • Backoffice staff in several hospitals can no longer do their work, leading to backlogs in administrative tasks, and problems with appointment scheduling and re-scheduling. • In several hospitals there is also spill-over to medical devices, disabling these devices, affecting patient care directly. • Extortion attempts of the hospital and many current and former patients.

Risk scenario 3 – High stress level

Pandemic/flu-spike context, DDoS attack, ransomware attack, ransomware spreading to several hospitals, affecting also IT environment and also medical devices, the online EHR system is unavailable, which disrupts both non-critical and critical care, patients have to be moved to other hospitals (cross-border dimension). Severe impact on both critical care and non-critical care, patients being moved to other hospitals, also across the border.

<table>
<tr><td colspan="2">Scenario 3: DDoS attack combined with ransomware outbreak affecting medical devices, non-critical and critical care

Pandemic/flu, DDoS, ransomware, online EHR system, regional crisis</td></tr>
<tr><td>Description</td><td>Impact</td></tr>
<tr><td>• Against a backdrop of a pandemic/flu-spike, when there is already pressure on hospital staff, due to lack of staff and a large number of patients.

• Attackers launch a DDoS attack, causing network outages, among other things affecting access to the national EHR system, which in turn affects the hospital’s health information system.

• Using the DDoS attack as a distraction, attackers launch a ransomware attack on an unpatched system in the hospital’s IT environment.

• Ransomware spreads rapidly and in some cases infects also medical devices in the hospital’s OT environment.</td><td>• Staff at targeted hospital can no longer access the internet, nor the national EHR system.

• All administrative back-office processes in the hospital come to a halt

• Ransomware disables several medical devices in the hospital, medical staff switch to other options.

• All non-critical patient care is affected, because health records and appointment schedules are not available. Even cancelling appointments is impossible.

• Hospital’s capacity to provide critical patient care is also affected and ambulances are re-routed and several patients have to be moved urgently.</td></tr>
</table>

Links to similar incidents reported in the media:

- In March 2023, Hospital Clínic de Barcelona suffered a cyberattack that forced it to cancel 150 interventions and between 2000 and 3000 external consultations. The amount of reported data involved in the ransomware attack as published was 4.5TB

https://govern.cat/salapremsa/notes-premsa/488382/ciberatac-al-clinic-afecta-seva-activitat-assistencial-habitual

- In May 2021, the HSE Health Service Executive (HSE), an organisation that provides all of Ireland's public health services through hospitals and communities across the country (with approximately 4,000 locations, 54 acute hospitals and over 70,000 devices), was subjected to a serious cyberattack through the criminal infiltration of their IT systems (PCs, servers, etc.) using Conti ransomware

https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

- In May 2024, Ascension Health fell victim to a Black Basta ransomware attack that disrupted clinical operations across the Catholic health system's 142 hospitals. The attack was detected on May 8, 2024, and resulted in an electronic health record outage that lasted for almost 4 weeks.

https://www.hipaajournal.com/ascension-cyberattack-2024/

- In February 2024, Change Healthcare fell victim to a ransomware attack (largest data breach in healthcare for 2024 - maybe even of all time) as a result of which patient care was indirectly affected (patients could not obtain medication unless they could pay out of pocket). It is estimated that 190m individuals were affected + the revenue of health care providers in the US

https://hyperproof.io/resource/understanding-the-change-healthcare-breach/

https://www.authmind.com/blog/critical-takeaways-change-healthcare-breach

b. Fixed networks

Risk scenario 1 – Low stress level (mandatory baseline scenario)

Scenario	Description	Potential Impacts	Map to Nevers related scenarios
Cable cut and BGP hijack	• Major land cable is cut or disconnected due to **accidental construction damage or sabotage**. • Simultaneously, a BGP hijack attack redirects traffic from a major ISP, causing traffic delay and **rerouting through a third country** before reaching its intended destination.	• **Regional internet disruptions** – Users in affected cities experience packet loss, slow speeds, or full outages. • **Traffic interception – Sensitive data was rerouted through third countries enabling surveillance and espionage** • **Limited cascading effects** – there is some impact in the digital infrastructure sectors and other sectors – some cloud services are affected, some failures in communications	• R6 – Coordinated physical sabotage attack on digital infrastructure • R10 – Interconnection attack to cause a large-scale network outage

Risk scenario 2 – Medium stress level

Scenario	Description	Potential Impacts	Map to Nevers related scenarios
Multiple cable cuts at IXPs, large scale DDoS attacks, compromised edge routers	• Unknown attackers carry out a coordinated physical sabotage attack cutting **multiple terrestrial cables at key**	• **Internet congestion & partial global blackouts** – nations or entire regions lose primary routes and must rely on overloaded alternative paths. • **Disrupted financial markets & cloud infrastructure** –	• R5 – DDoS attack to cause a large-scale network outage • R6 – Coordinated physical sabotage attack on

	interconnection points • Simultaneously, there are large scale DDoS attacks on the telecom sector. These attacks may be a diversion tactic. • At the same time, some telcos report a supply chain attack (network equipment vendor) on a large number of edge routers, as part of a pre-positioning attack. After threat information sharing, other telcos report similar issues with their routers. Response teams are already stretched and don't have time to investigate all their devices.	global stock markets, cloud computing providers, and banking networks face temporary outages due to connectivity failures	digital infrastructure • R10 – Interconnection attack to cause a large-scale network outage

Risk scenario 3 – High stress level

Scenario	Description	Potential Impacts	Map to Nevers related scenarios
Coordinated physical sabotage on land cables, massive DDoS attacks by botnets, cyber attacks disabling routers	• Unknown attackers carry out a coordinated physical sabotage attack cutting multiple terrestrial cables at key interconnection points • Weaponized botnets are used to launch massive DDoS attacks to flood telecom networks and other critical sectors. • Many telecom providers and IXPs are dealing with outages, because compromised edge routers are being disabled by attackers. An undetected cyber-attack, for the purpose of pre-positioning attack, was later used to disable critical core routers on a large scale.	• Internet traffic outages, latencies • Critical sectors affected, mainly hospitals and banks, are facing problems with their online services, and their payment services. • Public awareness: Telecom operators warn that communication may have been intercepted, and are advising users to use e2e communication apps.	• R4 – Third country interference on a supplier, MSP or submarine cable • R5 – DDoS attack to cause a large-scale network outage • R6 – Coordinated physical sabotage attack on digital infrastructure • R10 – Interconnection attack to cause a large-scale network outage

Links to similar cases reported in the media:

- https://www.axios.com/2024/07/29/france-fiber-optic-olympic-attack (coordinated cuts of land cables)
- https://therecord.media/finland-cert-reports-record-number-of-denial-of-service-attacks (large scale DDoS attacks in Finland)
- https://www.techtarget.com/searchsecurity/news/366619108/Salt-Typhoon-compromises-telecom-providers-Cisco-devices (large scale hacking of telco CISCO edge routers)
- Russian telco Rostelecom hijacks traffic for IT giants, including Google - BGP hijack
- BGP event sends European mobile traffic through China Telecom for 2 hours - Ars Technica - BGP hijack
- Nordic confusion over damage to Swedish-Finnish data cables - Euractiv - accidental cuts

c. Submarine cable infrastructures

Risk scenario 1 – low stress level (mandatory baseline scenario)

The scenario could include a combination of the following elements (or 'injects'), which can be adapted to the national context. Each element alone can be considered to have a moderate impact (2 out of 5) in accordance with the cyber-security risk assessment methodology by the NIS Cooperation Group:

- Mandatory: Cable cut in territorial waters/EEZ of an EU Member State affecting at least two EU Member States.
- Mandatory: Cyber intrusion into cable landing station where cables land that impact at least two EU Member States.
- Optional: Temporary shortage of maintenance vessels in EU waters.
- Optional: Temporary supply shortage of key components.

Risk scenario 2 – medium stress level

The scenario could include a combination of the following elements (or 'injects'), which can be adapted to the national context. Each element alone can be considered to have a substantial to critical impact (3 or 4 out of 5) in accordance with the cyber-security risk assessment methodology by the NIS Cooperation Group:

- Cable cut in territorial waters/EEZ of a third country affecting at least two EU Member States.
- Physical damage to beach manholes where cables land that impact at least two EU Member States.
- Physical damage to a maintenance vessel serving in EU waters or of a spares depot.

- Third country interference on supplier of key components (incl. cyber espionage) (corresponds to R2-4 Nevers Report).

Risk scenario 3 – high stress level

The scenario could include a combination of the following elements (or 'injects'), which can be adapted to the national context. Each element alone can be considered to have a critical to catastrophic impact (4 or 5 out of 5) in accordance with the cyber-security risk assessment methodology by the NIS Cooperation Group:

- Cable cut in high seas affecting at least three EU Member States.
- Physical intrusion into cable landing station where cables land that impact at least two EU Member States and destruction of equipment (including potentially the entire cable landing system).
- Power cuts to cause a regional network outage (corresponds to R9 in Nevers Report).
- Coordinated sabotage of several maintenance vessels serving the EU or of several spares depots.
- Block of supply (e.g., embargo) or backdoor access to system enabling malicious system shut down.
- Potential additional aggravation elements: natural disaster, accident

Links to similar cases reported in the media:

- 17 Nov 2024: Telia Lithuania cable between Lithuania and Sweden damaged
- 18 Nov 2024: C-Lion1 cable between Finland and Germany stopped working
- 25 Dec: Estlink-2 (submarine power cable connecting FI and EE) and four telecom cables damaged
- 26 Jan: Sweden-Latvia telecoms submarine cable damaged
- 21 Feb: New damage reported on C-Lion1 cable between Finland and Germany