DIGITAL Europe Programme - Cybersecurity

2022

#DigitalEuropeProgramme

"Europe's digital future can only succeed if people and businesses can be sure of the connected products and services we increasingly rely on."

Margrethe Vestager

Executive Vice-President for a Europe Fit for the Digital Age

Challenges in Cybersecurity

- Geopolitical contest over cyberspace
- Large increase in cybercrime
- Supply chain security (e.g., 5G)
- Expanding attack surface (e.g., IoT, eHealth, vaccine distribution)
- Advent of AI
- Vulnerability of smaller organisations, SMEs
- Info sharing, joint analysis and response
- Uptake

The EU's Cybersecurity Strategy for the Digital Decade

DIGITAL EUROPE PROGRAMME

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

Revised Directive on Security of Network and Information Systems (NIS 2)

Cybersecurity Shield (CSIRT, SOC)

Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS

Competence Centre and Network of Coordination Centres (CCCN)

EU workforce upskilling

BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

Cybersecurity crisis management framework

Cybercrime agenda

Member States' cyber intelligence

Cyber Defence Policy Framework

COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

EU leadership on standards, norms and frameworks in standardisation bodies

Promote Multi-Stakeholder Internet governance model

Cyber Capacity Building Agenda

EU Cyber Dialogue and Diplomacy Network

I. Sovereignty

IV. Cybersecure EU institutions

II. Capacity

III. Global and open
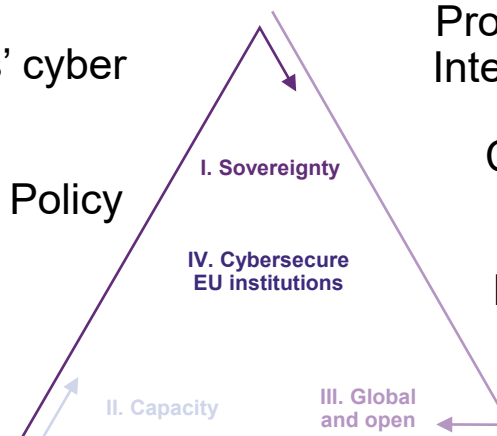
The ECCC and Network (NCCs)

EU Cybersecurity Competence Centre and Network

European Competence Centre
- Funds manager for cybersecurity in Digital Europe and Horizon Europe 2021-2027
- Facilitate the Network and Community to drive the cybersecurity technology agenda
- Support joint investment by the EU, Member States and industry

Network of National Coordination Centres
- Member States contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive and pass financial support
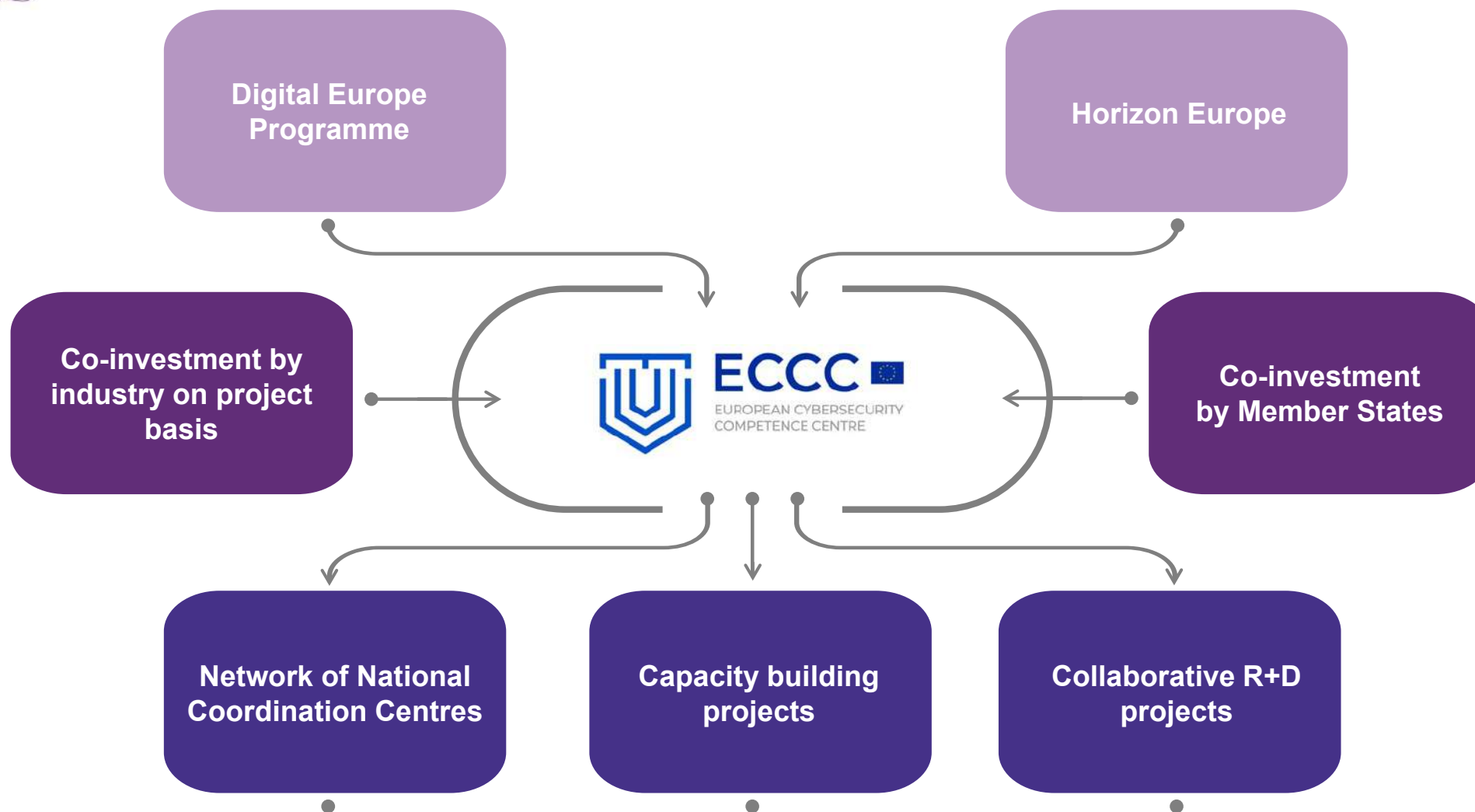
Community
- A large, open, and diverse group of cybersecurity stakeholders (research, private and public sectors, both civilian and defence)

Chip

Network of National Coordination Centres

One NCC per Member State	May receive/pass EU funding	Promotes participation in cross-border projects and in cybersecurity action	National capacity building and link with existing initiatives

Coordinates the national, regional and local levels	Promotes cybersecurity educational programmes	Advocates involvement of relevant entities

Competence Community

A large, open, and diverse group of cybersecurity stakeholders

Exchanges with the ECCC/NCCs on developments in cybersecurity

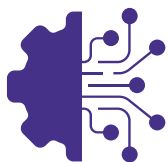Provides input to the activities of the ECCC/NCCs

Cybersecurity in DIGITAL

DIGITAL-CYBER-03

DIGITAL Europe Programme

1

Deployment of technology to businesses and citizens.

2

Speed up economic recovery and digital transformation of European economy and society.

3
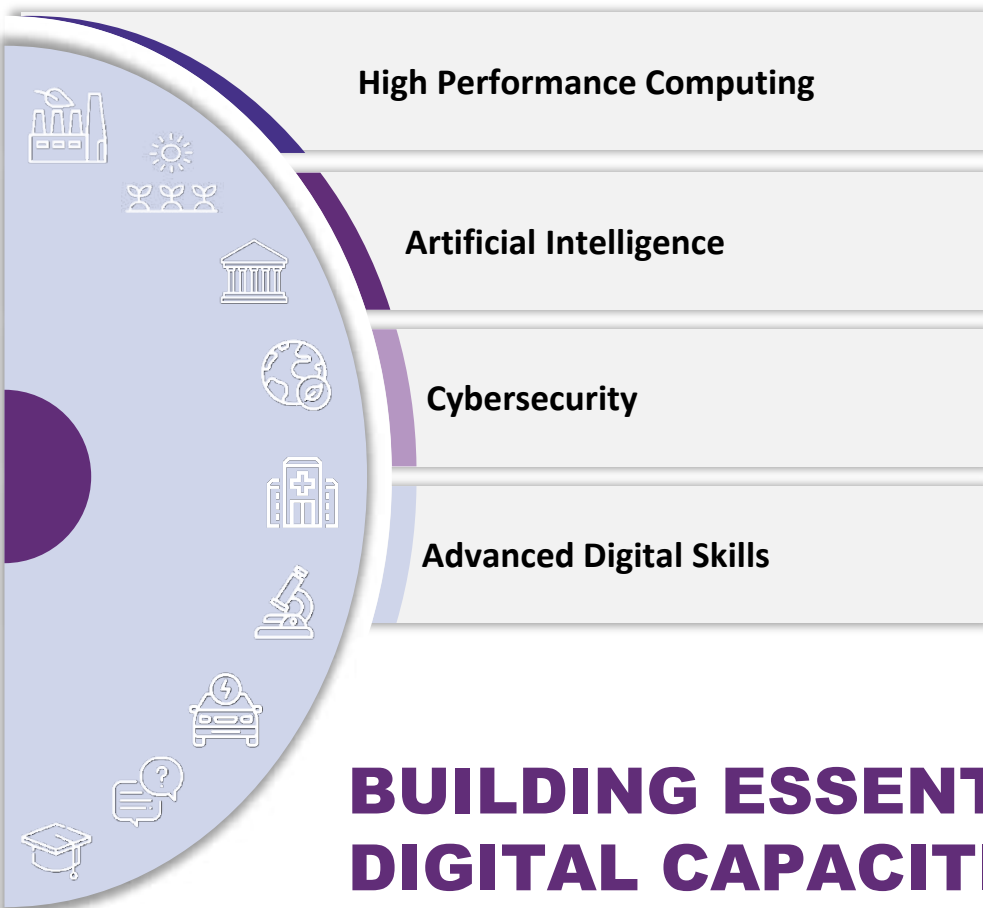
Complementary to other EU programmes, e.g., Horizon Europe

4

Strategic financing for five crucial areas

DIGITAL - Structure

High Performance Computing

Artificial Intelligence

Cybersecurity

Advanced Digital Skills

Digital Innovation Hubs

High Impact Deployments

BUILDING ESSENTIAL DIGITAL CAPACITIES

DIGITAL WP 2021-2022

European Cyber Shield

Resilience, coordination and cybersecurity ranges

SOCs

5G and digital infrastructures

Uptake of innovative cybersecurity solutions

Health sector cybersecurity

Support to Legislation

National Coordination Centres

Community *support*

NIS Directive implementation

Testing and certification

Other

EuroQCI

Advanced digital skills

Current call

DIGITAL-CYBER-03

Digital Europe: 2022 topics and deadlines

Topic	Budget (M€)	Opening	Deadline
Network of National Coordination Centres	33 + 22		
EU cybersecurity resilience, coordination and cybersecurity ranges	15		
Capacity building of Security Operation Centres (SOCs)	72.5 + 30		
Secure 5G and other strategic digital infrastructures and technology	10	15/11/2022	15/02/2023
Uptake of innovative cybersecurity solutions in SMEs	32		
NIS Directive implementation and national cybersecurity strategies	20		
Testing and certification capabilities	5		

Uptake of innovative cybersecurity solutions (I)

Objective (s)

- Market uptake and dissemination of innovative cybersecurity solutions
    - From SMEs and from EU-funded research
- Improve knowledge and auditing of cybersecurity preparedness

Scope

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

Uptake of innovative cybersecurity solutions (II)

Outcomes and deliverables

- Adoption of market-ready innovative cybersecurity solutions
- Provide and deploy up to date tools and services to organisations (In particular SMEs)
- Improve the security of open source solutions

KPIs to measure outcomes and deliverables

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

SMEs and other organisations

SME support grant (75% co-funding rate for SMEs), EUR 32M, 1-5M per grant, 36mos

Deploying the Network of National Coordination Centres with Member States

Objective(s)

- NCCs will support cybersecurity capacity building at national and, where relevant, regional and local.
- Foster cross-border cooperation and at the preparation of joint actions.

Scope

- Proposals are expected to further specify the activities mandated by the ECCC Regulation and possibly others
- Proposals are expected to demonstrate possible coordination with relevant European Digital Innovation Hubs

Outcomes and deliverables

- Setup and operation of National Coordination Centres in Member States.

Capacity building of Security Operation Centres (SOCs) (I)

Objective(s)

- Create, interconnect and strengthen cyber threat detection capacities
  - To monitor and detect cyber threats, the creation of collective knowledge and sharing of best practices
- CTI data and capacities brought together through cross-border platforms across the EU
- Use of state-of-the-art AI, machine learning capabilities and common infrastructures
  - To more efficiently and rapidly share and correlate the signals detected, and to create high-quality threat intelligence

Scope

- Proposals should focus on at least one of the following
  - Supporting entities providing cyber threat detection services
  - Strengthening such entities by leveraging state of the art AI
  - Supporting information sharing
  - Developing and deploying appropriate tools, platforms and infrastructures to securely share and analyse large sets of CTI.
  - Supporting the increased availability, quality, usability and interoperability of threat intelligence data among relevant entities.

Capacity building of Security Operation Centres (SOCs) (II)

Outcomes and deliverables

- World-class cyber threat detection capacities across the Union, strengthened with state of the art technology in areas such as AI
- Sharing of CTI
- CTI and situational awareness capabilities supporting strengthened collaboration in the framework of the Blueprint/CyCLONe
- Cross-border platforms for pooling CTI between several Member States with highly secure infrastructures and advanced data analytics tools

KPIs to measure outcomes and deliverables

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

Public and private actors which can support cyber threat detection and CTI sharing

Simple grant, EUR 72.5M, 1-10M per grant, 36mos, financial support to third parties

EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges (I)

Objective(s)

- Proposals should address at least one of the following objectives
    - Strengthen capacity to monitor cyberattacks and threats and supply chain risks, and to react jointly against large incidents.
        - Through the implementation of the Blueprint and considering the role of the CSIRT network and of CyCLONe.
    - Create, interconnect and strengthen cybersecurity ranges at European, national and regional level
        - In view to develop cybersecurity skills and expertise.

Scope

- First objective. E.g., aim to provide stakeholders with structured test methodologies, vulnerability databases and forensic tools, or automated content delivery.
- Second objective. Cybersecurity skills and expertise in key technologies (e.g. 5G, IoT, cloud, or AI) as well as application sectors (e.g. health, energy, finance or transport).

Outcomes and deliverables

- Capacity to react in a coordinated way to large scale cybersecurity incidents.
- Top-level cybersecurity ranges offering advanced skills, knowledge and testing platforms.

KPIs to measure outcomes and deliverables

- Regarding the first objective:
  - Report on interactions between the beneficiary(ies) and other stakeholders like peers or CSIRTs.
  - …
- Regarding the second objective:
  - Number of cyberranges created.
  - Number of cyberranges interconnected.
  - Maturity analysis pre and post implementation to measure the change in capacity of the cyberranges of the beneficiary(ies).
  - …

All EU organisations with needs in cybersecurity and EU creators and providers of Cybersecurity Range services

SME support grant (75% co-funding rate for SMEs), EUR 15M, 1-4M per grant, 36mos, financial support to third parties

Supporting the NIS Directive implementation and national cybersecurity strategies (I)

Objective(s)

- Development of trust and confidence between Member States
- Effective operational cooperation of organisations entrusted with Cybersecurity
- Better security and notification processes
- Improved security of network and information systems in the EU
- More alignment and harmonisation of Member States' implementations of the NIS Directive

Scope

- At least one of
  - User-centred implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring, preventing, detecting and handling cybersecurity incidents
  - Collaboration, communication, awareness-raising activities, knowledge exchange and training, including using cybersecurity ranges, of public and private organisations working on the implementation of the NIS Directive
  - Twinning schemes involving originator and adopter organisations from at least 2 different Member States
  - Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs

Supporting the NIS Directive implementation and national cybersecurity strategies (II)

Outcomes and deliverables

- Enable the Member States to limit the damage of cybersecurity incidents, while reducing the overall costs of cybersecurity.
- Improve compliance with the NIS Directive, higher levels of situational awareness and crisis response.
- Contribute to enhanced cooperation, preparedness and cybersecurity resilience of the EU.

KPIs to measure outcomes and deliverables

- Number of actions performed to develop trust and confidence between Member States.
- Number of twinning schemes and their actual use.
- Improvement in compliance with the NIS Directive by the beneficiary(ies).
- …

Member State competent authorities, CSIRTs, OES, ISACs… (Minimum 3 different ones)

SME support grant (75% co-funding rate for SMEs), EUR 20M, 1-5M per grant, 36mos

Securing 5G Strategic Digital Infrastructures And Technologies (I)

Objective(s)

- Support relevant entities in Member States in the implementation of their national cybersecurity strategies and legislation in line with European 5G cybersecurity policy
- Support knowledge and capacity building for relevant national authorities

Scope

- At least one of
  - Support to 5G cybersecurity. Contribute to the goals and measures of the Recommendation and "toolbox" on 5G cybersecurity
  - Piloting and supporting capacity building of security and interoperability aspects of open, disaggregate and interoperable technology solutions

Securing 5G Strategic Digital Infrastructures And Technologies (II)

Outcomes and deliverables

- Trusted and secure 5G services.
- Cooperation between national authorities and private providers, in particular innovative European SMEs, on piloting, testing and integration of security and interoperability aspects of 5G interoperable, open and disaggregate solutions.

KPIs to measure outcomes and deliverables

- Number of Member States which received funding, with a clear national legislative framework implementing the EU 5G Toolbox in place.
- Number of knowledge and capacity building activities…
- Number of knowledge and capacity building activities related to security and interoperability aspects of innovative solutions…
- Number of test-beds, pilot projects on 5G interoperable, open and disaggregate solutions, such as Open RAN

All stakeholders, in particular national authorities (such as regulators of electronic communications)

Simple grant, EUR 10M, 1-3M per grant, 12-36mos, financial support to third parties

Testing and Certification Capabilities (I)

Objective(s)

- Increase and facilitate security and interoperability testing capabilities and certification of connected ICT systems.
- Improve the capabilities and cooperation of stakeholders in line with the objectives of the Cybersecurity Act.

Scope

- At least one
    - Support capacity building for national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies
    - Support SMEs to test and certify ICT products, ICT services or ICT process they sell
    - Provide support for SME users of ICT equipment to audit their infrastructures
    - Support standardisation actions considering activities by European and international standardisation organisations as appropriate
    - Support cyber-security and interoperability testing capabilities on 5G disaggregated and open solutions.

Testing and Certification Capabilities (II)

Outcomes and deliverables

- Strengthen national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies
- Improve the cybersecurity and interoperability testing capabilities in all MSs
- Support SMEs to audit their infrastructure in view of improving their cybersecurity protection
- Support actions in the area of standardisation

KPIs to measure outcomes and deliverables

- Additional certification and testing services provided by a beneficiary as a result of the activities
- Standardisation actions with European and international standardisation organisations that were supported
- ICT equipment's audits in terms of cybersecurity resilience by SMEs which were supported
- Cybersecurity and interoperability testing capabilities supported on 5G disaggregated and open solutions or on chips
- …

National cybersecurity certification authorities, conformity assessment and accreditation bodies, universities and other relevant stakeholders

Grants for Financial Support (100% funding rate), EUR 5M, 0.5-1M per grant, 36mos

Link to HE calls and topics

Increased cybersecurity 2022 (HORIZON-CL3-2022-CS-01)

- Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures
- Trustworthy methodologies, tools and data security by design for dynamic testing of potentially vulnerable, insecure hardware and software components
- Transition towards Quantum-Resistant Cryptograph
- Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

Increased cybersecurity 2021 (HORIZON-CL3-2021-CS-01)

- Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity
- Improved security in open-source and open-specification hardware for connected devices
- AI for cybersecurity reinforcement
- Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

Call document - Support to proposers

- Details on **admissibility and eligibility**
- Information for applicants on **financial and operational capacity**
- Exclusion criteria
- **Evaluation procedure**
- Guarantees, obligatory milestones and deliverables, certificates and any many other description on legal conditions to participate in grants
- Financial support to third party schemes and conditions
- All the **mandatory annexes** needed for the call (e.g. ethic issues, security issues)
- **Type of action** description
- Other important legal and operational provisions
- **Help for applicants** and how to reach out to the commission

Award criteria

Relevance

- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Reinforcement of the Union's digital technology supply chain*
- Resilience to financial obstacles*

Implementation
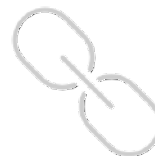
- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work

Impact
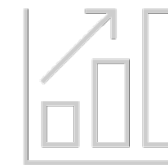
- Achievement of the expected outcomes and deliverables,
- as well as communication and dissemination
- Competitiveness strengthen and contribution to society
- Environmental sustainability*

* call document sets applicability

Budget categories and cost eligibility (I)

A. Personnel costs

- A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons and 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

Restrictions due to security:

- Subcontracted work must be performed in the eligible countries
- Only costs for activities carried out in eligible countries are eligible

Other cost categories. Costs for financial support to third parties (FSTP)

- Allowed for grants: CYBER-RESILIENCE, SOC, 5G-INFRASTRUCTURE, NAT-COORDINATION, TEST-CERT-CAPABILTIES
- Maximum amount per third party EUR 60000, unless a higher amount is required duly justified in the Application Form (100 000 for TEST-CERT-CAPABILITIES)

Proposal to provide:

- why FSTP is needed,
- how it will be managed,
- a list of the different types of activities that can receive support, and
- the results to be obtained.

FSTP grants under the following conditions:

- the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality,
- the calls must be published on the Funding & Tenders Portal, and on the participants' websites,
- the calls must remain open for at least two months,
- if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change, and
- the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries,
- the calls must have a clear European dimension.

Lessons learnt

- Study the Work programme and the Call document
- Fulfil the admissibility and eligibility requirements, e.g., completeness, readability, consortium composition, number of pages…
- Participation restrictions (Art. 12.5)
- Familiarise with the concept
- Fill accurately the self-declaration
- Ensure proposal is in scope
- Remember that proposals are evaluated as submitted!

Funding & tender portal

Useful links

Digital Europe Programme website
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Digital Europe Programme Regulation
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377

Funding & tender opportunities portal
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

Thank you