Cluster 3: Civil Security for Society

Destination
“Increased cybersecurity and a more secure online environment”

CALL “INCREASED CYBERSECURITY” (CS)

HORIZON-CL3-2024-CS-01

European Commission

Destination “Increased cybersecurity and a more secure online environment (CS)”

- **Expected impact of the Horizon Europe Strategic Plan 2021-2024:**
  - ***Increased cybersecurity*** *and a* ***more secure online environment*** *by developing and using effectively EU and Member States’ capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.*
- **Specific impacts:**
  - **Generate knowledge and value** in cross-cutting matters in order to avoid sector-specific bias and to **break silos** that impede the proliferation of common security solutions;
  - **Strengthen key pillars** of the research and innovation cycle to increase the effectiveness and efficiency of its contribution to the development of security capabilities;
  - **Support innovation uptake and go-to-market strategies** with the aim of paving the way towards an increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research, thus contributing to reinforce the competitiveness of EU security industry and safeguard the security of supply of EU products in key security areas.

European Commission

Destination “Increased cybersecurity and a more secure online environment (CS)”

- **CL3 Increased Cybersecurity:**
  - Will support the implementation of the **EU Cybersecurity Strategy.**
  - Will support the Regulation of the European Parliament and of the Council establishing the **European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)** and the Network of **National Coordination Centre (NCC)** (COM 2018(630))
  - Supported by R&I, citizens, public authorities and companies, including SMEs, will be empowered to **protect their data and online activities**, via a resilient critical digital infrastructure, both private and public, that better protects the Digital Single Market and the digital life of citizens against malicious cyber activities.
  - Will strengthen European cybersecurity industrial capacities, supply chain security and increased open strategic autonomy vis-à-vis foreign technologies.
  - Will support the use of **innovative digital technologies**, including self-healing, artificial intelligence, cryptography, massively distributed computing and storage, as well as quantum technologies to increase data security and augment cybersecurity.
  - Will support innovations in secure hardware and software development and implementation and improve methods for cybersecurity testing and certification

Destination “Increased cybersecurity and a more secure online environment (CS)”

- All these measures aim at **defending the integrity of the Digital Single Market** as well as the EU’s high standards concerning rights to privacy, protection of personal data, and the protection of other fundamental rights in the digital age on the global stage.

- The Destination will pay particular attention to the **cybersecurity of the most vulnerable organisations and individuals**.

- In order to defend against cyber-threats, the architectural principles of **‘security-by-design’ and ‘privacy-by-design’ will be implemented in digital technologies and their applications**, such as 5G, industry 4.0, artificial intelligence, Internet of Things, block chain, quantum technologies, mobile devices and connected cooperative and autonomous mobility and energy.

- Complementary Instrument: **Digital Europe Programme** (which focuses more on the industry side).

- Related policy areas: Quantum research, Cryptography, Support for cyber capacities and deployment, European Cybersecurity Competence Centre, NIS2 Directive, 5G, AI, Cyber Resilience Act, Cybersecurity Act, Cyber Solidarity Act, Certification, EU Cybersecurity Skills Academy, CyberCommunity

Overview

Topic	Instrument	EUR (million)	Projects	Opening date	Deadline date
Increased Cybersecurity (CS)					
CS01 - Approaches and tools for security in software and hardware development and assessment					
HORIZON-CL3-2024-CS-01-01	IA	37,00	6	27/06/2024	20/11/2024
CS02 –Post-quantum cryptography transition					
HORIZON-CL3-2024-CS-01-02	RIA	23,40	4	27/06/2024	20/11/2024

Destination “Increased Cybersecurity (CS)”

CALL TOPICS 2024

European Commission

HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment

➢ **Projects' results are expected to contribute to some or all of the following outcomes**:

- Improved hardware and software security engineering; resilient systems design;
- Improved access to testing of hardware and software in virtual, closed and secure environments;
- Systematic and, where possible, automated study of vulnerabilities, software analysis, vulnerability discovery, and dynamic security assessment;
- Trustworthy certifiable hardware and software;
- AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.

HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition

- **Projects' results are expected to contribute to some or all of the following outcomes:**
  - Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation;
  - Easy-to-use tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state-of-the-art standards;
  - Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms;
  - Phase-in of post-quantum algorithms or protocols to new or existing applications;
  - Demonstrators and good-practice implementations of post-quantum cryptographic algorithms on varied hardware and software platforms;
  - Application-oriented recommendations for the widespread implementation of post-quantum cryptography across the EU.

General conditions for call: Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)

General conditions

1. Admissibility conditions: described in Annex A and Annex E of the Horizon Europe Work Programme General Annexes

2. Eligible countries: described in Annex B of the Work Programme General Annexes

A number of non-EU/non-Associated Countries that are not automatically eligible for funding have made specific provisions for making funding available for their participants in Horizon Europe projects. See the information in the Horizon Europe Programme Guide.

3. Other eligibility conditions: described in Annex B of the Work Programme General Annexes

4. Financial and operational capacity and exclusion: described in Annex C of the Work Programme General Annexes

5. Award criteria, scoring and thresholds are described in Annex D of the Work Programme General Annexes

6. Submission and evaluation processes are described in Annex F of the Work Programme General Annexes and the Online Manual

7. Indicative timeline for evaluation and grant agreement: described in Annex F of the Work Programme General Annexes

8. Legal and financial set-up of the grants: described in Annex G of the Work Programme General Annexes

Additional documents

✓HE Main Work Programme 2023–2024 – 1. General Introduction

✓HE Main Work Programme 2023–2024 – 6. Civil Security for Society

✓HE Main Work Programme 2023–2024 – 13. General Annexes

✓ HE Programme Guide

✓HE Framework Programme and Rules for Participation Regulation 2021/695

✓HE Specific Programme Decision 2021/764

✓EU Financial Regulation

✓EU FTP Q&A (Horizon)

Thank you!

European Commission