



Horizon Europe – Work Programme 2026/2027

Cluster 3 Civil Security for Society - Destination Cybersecurity

Indicative Budget

€128 million



Indicative Number
of Projects

33

Key Features for both the 2026 and 2027 Work Programmes

- **Management model:** Unlike the other destinations under Cluster 3, Cybersecurity will be **Indirectly managed** by the **European Cybersecurity Competence Centre (ECCC)**
- **Funding form:** Lump-sum grants (new effort by EC to simplify implementation)
- **Eligibility:** Limited to legal entities established in EU Member States or Horizon Europe Associated Countries (UK Associated January 2024) **Please note** entities controlled directly or indirectly by non-eligible countries are excluded from these calls!
- **Security sensitivity:** Some activities may involve EU Classified Information (EUCI) or sensitive results (SEN)

Across both years, the programme aims to:

- ✓ Strengthen **EU cybersecurity capability and resilience**
- ✓ Secure **critical digital supply chains**
- ✓ Enable **trustworthy AI and post-quantum readiness**
- ✓ Protect **strategic EU interests and technological sovereignty**

The Call Topics 2026 – A Summary

Calls Open: 3 March 2026

Submission Deadline: 15 September 2026

Call Topic: HORIZON-CL3-2026-02-CS-ECCC-01 - Approaches and tools for security in software and hardware development and assessment

- **Type:** Research and Innovation Action (RIA)
- **Budget:** €20 million
- **EU contribution per project:** €3–4 million
- **Expected projects:** 4–5

Focus areas:

- Secure hardware (trusted chips, tamper-resistant architectures, secure boot)
 - Hardware and software supply chain security
 - Security-by-design methodologies
 - AI-driven and formal verification security testing
 - Post-quantum cryptography (PQC) in hardware and firmware
 - Self-healing firmware and automated recovery mechanisms
-

Call Topic: HORIZON-CL3-2026-02-CS-ECCC-02 - SecureAI – Security, Privacy and Robustness of AI Systems

- **Type:** Innovation Action (IA)
- **Budget:** €21.2 million
- **EU contribution per project:** €3–4 million
- **Expected projects:** 4–5

Focus areas:

- Robust AI models resistant to adversarial attacks
 - Detection and mitigation of data poisoning and backdoors
 - Privacy-preserving AI (federated learning, secure aggregation, homomorphic encryption)
 - Trusted AI deployments for government and enterprise
 - Alignment with the EU AI Act
-

Call Topic: HORIZON-CL3-2026-02-CS-ECCC-03 - Advanced Cryptography and High-Assurance Implementations

- **Type:** Research and Innovation Action (RIA)
- **Budget:** €15 million
- **EU contribution per project:** €2–3 million
- **Expected projects:** 3–4

Focus areas:

- Post-quantum cryptographic schemes (including non-lattice approaches)
 - Digital wallets, eIDs and authentication protocols
 - High-Assurance Cryptographic Software (HACS)
 - Formal verification and machine-checked security guarantees
-

The Call Topics 2027 – A Summary

Call Topic: HORIZON-CL3-2027-02-CS-ECCC-01 - AI for Cybersecurity Applications

- **Type:** RIA
- **Budget:** €24.8 million
- **EU contribution per project:** €4–5 million
- **Expected projects:** 5–6

Focus areas:

- AI-driven real-time threat detection
 - Adaptive and explainable AI defence systems
 - AI-enabled Security Operations Centres (SOCs)
 - Trustworthy and resilient AI under the AI Act
-

Call Topic: HORIZON-CL3-2027-02-CS-ECCC-02 - Secure Computing Continuum (IoT–Edge–Cloud–Data Spaces)

- **Type:** Innovation Action (IA)
- **Budget:** €24 million
- **EU contribution per project:** €3–4 million
- **Expected projects:** 5–6

Focus areas:

- End-to-end security from IoT to cloud
 - Zero-trust architectures
 - Privacy-preserving data sharing (GDPR-compliant)
 - PQC acceleration and SW/HW co-design
 - Interoperability across computing layers
-

Call Topic: HORIZON-CL3-2027-02-CS-ECCC-03 - Secure PQC Implementations and Post-Quantum Digital Trust

- **Type:** RIA
- **Budget:** €19 million
- **EU contribution per project:** €3–4 million
- **Expected projects:** 4–5

Focus areas:

- Side-channel and fault-attack resistant PQC implementations
 - Formal verification and automated evaluation tools
 - Cryptanalysis and quantum hardness analysis
 - Post-quantum digital identity and privacy-friendly services
-

Call Topic: HORIZON-CL3-2027-02-CS-ECCC-04 - New Primitives for Hybrid Classical-Quantum Networks

- **Type:** RIA
- **Budget:** €4 million
- **EU contribution per project:** €4 million
- **Expected projects:** 1–2

Focus areas:

- Cryptographic primitives beyond QKD
 - Hybrid classical–quantum security protocols
 - Fundamental research linking quantum information and cryptography
 - Roadmap for future quantum cryptography and networks
-