# EN

# Horizon Europe

# Work Programme 2026-2027

## *6. Civil Security for Society*

# Table of contents

# Introduction

Cluster 3 provides a research and innovation response to a context of rapidly changing threats and challenges to internal security, the security of citizens, critical infrastructure and the security of society as a whole. These threats are driven by geopolitical, technological and societal changes, including:

- Instability, hybrid threats and the resurgence of war on the European continent, in particular the Russian war against Ukraine, making the need for civilian protection, preparedness, and resilience.
- Continued threat from terrorism and increased threat from organised crime.
- The potential for large-scale movements of people, whether as a result of war, the instrumentalisation of migration or other drivers, require effective border management capabilities and further efforts to combat migrant smuggling, trafficking in Human Beings (THB), and possible terrorist infiltration.
- More frequent and serious climate-related extreme events as well as other disasters, whether accidental or intentional, of human or natural origin, requiring disaster risk management and response.
- Continued technological development and digitalisation create new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists, as well as new challenges, needs and opportunities for security practitioners.
- Cyber threats that put infrastructures, businesses, public administrations, and individuals at risk.
- Negative socio-economic trends and climate adaptation that create potential for greater social polarisation and mistrust, which may escalate into conflict and/or create opportunities for extremists and malicious actors to spread hate speech and foreign information manipulation and interference and disinformation.

In addressing these and their related challenges, through research and innovation, this Work Programme will support the implementation of the new ProtectEU – European Internal Security Strategy[1] and European Preparedness Union Strategy[2] and the sectoral strategies, legislation and action plans identified in the **Destinations**.

Each Destination includes an introductory section that explains the relevant policy objectives, specifies elements to be taken into account for the topics of the Destination and identifies specific expected impacts. Proposals should set out a credible pathway to contribute to the specific expected impacts:

1 COM/2025/148 final.
2 JOIN(2025), 130 final.

- **Better protect the EU and its citizens against Crime and Terrorism (FCT)**

*Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 13 "Tackling crime and terrorism more effectively and increasing the resilience of infrastructures".

- **Effective management of EU external borders (BM)**

*Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 12 "Facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts".

- **Resilient infrastructure (INFRA)**

*Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 13 "Tackling crime and terrorism more effectively and increasing the resilience of infrastructures".

- **Disaster-Resilient Society for Europe (DRS)**

*Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 11 "Reducing losses from natural, accidental and human-made disasters".

- **Strengthened Security Research and Innovation (SSRI)**

*Link to the Horizon Europe strategic plan 2025-2027:* Cross-cutting Destination that supports all the Expected impacts identified above.

In addition, under this Work Programme, the Commission intends to entrust implementation of a call for proposals to the European Competence Centre for Cybersecurity (ECCC). The call topics foreseen for this indirectly managed action (see Appendix to this Work Programme part) relate to:

- **Cybersecurity (CS)** *Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 14 "Increasing cybersecurity and making the online environment more secure".

Cluster 3 Work Programmes will support the implementation of the European Commission political guidelines 2024-2029 for a 'Safer and more secure Europe', a 'Preparedness Union', with 'Stronger Common Borders', protecting democracy and putting research and innovation at the heart of a resilient economy. Overall, research under this Cluster should continue to focus on preserving and securing **citizens' basic right to feel safe.** Cluster 3 'civil security for society' will therefore also support the Commission's work:

- the new European Internal Security Strategy, fighting organized crime and ensuring that security is integrated in EU legislation and policies by-design.

- towards a European Civil Defence Mechanism, looking at all facets of crisis and disaster management, along community resilience building.

- to provide practitioners, law enforcement authorities including customs fand border guards, first and second responders, critical infrastructure operators, with adequate and

up-to-date tools for lawful access to digital information, while safeguarding fundamental rights.

- to strengthen European competitiveness and make better use of public procurement and in particular support innovation procurement.

Successful projects need to show their understanding of and contribution to a wider innovation cycle based on a needs-driven capability development approach that triggers research, steers its implementation and capitalises on its outcomes. This means that projects need to show, on the one hand, an understanding of the capability requirement and policy context that has led to the R&I need, and, on the other hand, a strategy for ensuring the uptake of the outcomes including opportunities where relevant for using EU funds for deployment.

Eligibility to participate is also subject to the 'Participation of Chinese universities linked to the Ministry of Industry and Information Technology (MIIT)' eligibility condition (see General Annex B of the General Annexes).

**Cross-cutting themes**

Various themes run through this Work Programme, cutting across the different sectoral Destinations. A first set of themes respond to the wider challenges identified in the three key strategic orientations of the Horizon Europe strategic plan 2025-2027:

- *Strengthening resilient societies and democracy.* The central focus of Cluster 3 is to support through research and innovation, the prevention, preparedness and response to the wide range of threats to internal security identified above, as well as ensuring the security of all citizens, critical infrastructure, supply chains and of society as a whole. Strengthening our democracies and making them more resilient – both materially and psychologically – has taken on a new urgency since the full-scale Russian invasion of Ukraine. European citizens need to be protected from hybrid threats such as disinformation and foreign information manipulation and interference campaigns while upholding the rule of law and basic freedoms, including freedom of speech. Civil security research and innovation needs to equip civil security practitioners, such as law enforcement, with the ability to mitigate the consequences of armed conflict, in particular attacks on critical infrastructures. By funding research to strengthen and prepare our societies, democracies, and infrastructure against hybrid threats, Cluster 3 shows its ability to adapt to changing conditions and challenges and mitigate the consequences of armed conflict, in particular attacks on critical infrastructures. By funding research to strengthen and prepare our societies, democracies, and infrastructure against hybrid threats, Cluster 3 shows its ability to adapt to changing conditions and challenges.

- *Securing the digital transition*. The more widespread and ubiquitous digital technology is, the greater the threats of new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists as well as new challenges, needs and tools for law enforcement authorities, infrastructures, businesses and individuals. Research on

cybercrime and cybersecurity helps to address these matters. With the aim of creating a secure and trustworthy digital environment, Cluster 3 will invest in cybersecurity R&I to strengthen the EU's resilience, protect its infrastructures and improve its ability to cope with cyber incidents. This will help increase the EU's open strategic autonomy in cybersecurity. Cluster 3 addresses cybercrime and the developing security threats in a digital age, such as criminal use of AI, to protect people, institutions and companies against cyber-enabled crimes. It will also continue to harness the opportunities of new technologies for law enforcement, border management and disaster risk reduction and uphold the ability of the law enforcement to lawfully access and exploit digital evidence, without compromising or weakening privacy safeguards or cybersecurity.

- *Supporting the green transition in civil security*. Climate change and environmental degradation are increasingly recognised as threat multipliers. Climate-related extreme events such as floods, droughts and forest fires pose increasing threats to people, nature business and infrastructure. Geological hazards such as earthquakes, volcanic eruptions, and tsunamis are also threats affecting security. As EU Member States and Associated Countries face similar challenges, *including varied and evolving transnational* disasters, Cluster 3 will develop solutions to be applied throughout the EU to keep up to date with the developments. Cluster 3 will also address environmental crime. It will help understand how to manage borders in case of potential large-scale movements of people, including those caused by environmental stress. It will promote environmental sustainability of security solutions.

A second set of cross-cutting themes respond to challenges more specific to Cluster 3:

- *Ensuring legal and ethical outcomes that are supported by society*. Ethics, respect for the rule of law, fundamental rights, including human rights, privacy and the protection of personal data, as well as responsible research, must be at the heart of security research. Citizens and communities, including women and underrepresented groups, should be engaged, for example in assessing the societal impact of security technologies, to improve the quality of results and to build public trust. Social sciences and humanities (SSH) and social innovation need to be appropriately integrated into security research. The aim is to develop an inclusive set of civilian security solutions that are as minimally intrusive as possible while respecting freedoms, rights and values.

- *Protecting and empowering disadvantaged groups or in a vulnerable situation*. A range of groups are disproportionately exposed to violence and threats towards their security. These include, women, LGBTIQ people, ethnic, racial or religious minorities, persons with a migrant background, persons with disabilities[3], persons living with chronic illnesses, older people and children. The vulnerability of these groups is further exacerbated by factors such as insecure supply chains for essential medicines which can

[3] In line with the UNCRPD, the EU has a long-standing commitment to provide humanitarian aid that is inclusive and accessible to persons with disabilities. Situation of persons with disabilities in the case of meteorological, hydrological, geophysical events and armed conflicts needs to be specifically addressed by ensuring a truly inclusive preparedness where persons with disabilities are provided with the right tools on how to act in emergencies.

be disrupted by disasters or criminal activities. The needs and rights of travellers, migrants, and refugees must be protected and promoted in border management activities. Unfortunately, these groups are also at a higher risk of falling victim to trafficking in human beings. Research under Cluster 3 needs to consider how these groups can be better protected, including by analysing the structures that foster violence against these groups, developing measures to tackle violence, and promoting inclusive and empowering approaches that prioritise the needs and the rights of disadvantaged groups or in a vulnerable situation.

- *Improving market uptake of civil security research solutions*. Despite many success stories of tools and capabilities used by security practitioners originating from EU-funded security research projects, the uptake and deployment of successful research results remains a constant challenge. This challenge spans all destinations.

This Work Programme:

- continues the Cluster 3 practice of requiring projects to involve security practitioners, such as law enforcement, alongside researchers and industry. Such involvement has shown its added value in ensuring that tools, technologies and capabilities are developed for the benefit of and use by end-users and practitioners;

- strengthens this involvement by introducing in many topics a requirement that proposals should plan a mid-term deliverable where practitioners involved in the project assess the project's mid-term outcomes;

- innovation procurement is used under the SSRI destination, this year with the open grounds preparatory work for future Pre-Commercial Procurement (PCP) topic, to bridge the gap between research, innovation and deployment, and thus strengthen the European market and European civil security industrial base;

- encourages synergies with other EU funding programmes and instruments to enable or facilitate the uptake of the results of research into deployable solutions. Further information about this is given below.

- the possibilities and support of security end-users like FRONTEX, EUROPOL, EU-LISA, the EU Drugs Agency and the proposed EU Customs Authority (in the context of the Customs Reform), for testing and validation of security research results should be used and expanded to the fullest extent.

- supports projects which can directly or indirectly support public institutions intent on setting up their own innovation processes, which is to be encouraged.

- encourages a competitive and innovative market, accessible for small and medium-sized enterprises (SMEs).

Where relevant, Cluster 3 will make use of space technology and Earth Observation.

A third set of cross-cutting themes address the need for greater simplification and research and innovation funding in support of the EU's competitiveness:

- *Strengthening European competitiveness*. Growing challenges, such as climate change, artificial intelligence and geopolitical tensions are changing the world we live in. It is therefore paramount that Europe is a place where growth and innovation continue to be fostered. To do so, competitiveness has been placed at the heart of the EU's economic agenda. The Commission's work in this area is guided by the Competitiveness Compass and the Draghi report. Cluster 3 will contribute to increasing Europe's competitiveness through research and innovation projects which contribute to the development of key technologies, reduce dependencies and further strategic autonomy, increase resilience and security, and preserve and secure citizens' basic right to feel safe.

- *Increased simplification.* In order to simplify applying for funding and taking part in the programme certain measures have been applied, these include topics that are more open and adequately prescriptive, and the application of lump sum funding.

**International cooperation**

Cluster 3 continues to require a specific approach to international cooperation to achieve the right balance between the benefits of exchange with key international partners, while ensuring the protection of the EU's security interests and the need for strategic autonomy in critical sectors.

Under the destination 'Disaster-Resilient Society for Europe' (DRS), there is an established culture of comprehensive research collaboration with non-EU countries, taking account of the transnational aspect of different natural and human-made hazards and their causes (such as climate change). Therefore, under this destination, international cooperation is strongly encouraged, given the value of international cooperation, especially in developing technologies for first responders.

For the destinations relating to border management, the fight against crime and terrorism, infrastructure resilience and cybersecurity, international cooperation will be explicitly encouraged only where appropriate and specifically supportive of ongoing collaborative activities.

**Synergies with other EU funding programmes and instruments**

Cluster 3 will continue building and facilitating synergies with other EU funding programmes and instruments, in an approach with long-term capability development planning at its core. This is particularly important for civil security, where solutions are often demand-driven in a market that tends to be narrow, institutional, highly regulated, sensitive, and often fragmented along national lines.

From the demand side (funding for security practitioners and authorities, who are the users of security solutions), Cluster 3 will continue to operationalise the synergies with the home affairs funds: the Internal Security Fund (ISF) and the Integrated Border Management Fund

(IBMF) in its two components, the Border Management and Visa Instrument (BMVI) and the Customs Control Equipment Instrument (CCEI). This will mean both facilitating the uptake of the results of Cluster 3 research by Member States and Associated Countries in their national programmes, and programming EU and specific actions with funding dedicated to taking up innovation resulting from Cluster 3 research.

In addition to the home affairs funds, Cluster 3 will continue promoting synergies with the Digital Europe Programme, the European Maritime Fisheries and Aquaculture Fund (EMFAF), the Union Civil Protection Mechanism (Knowledge for Action in Prevention and Preparedness calls for proposals, rescEU grants, early warning capabilities, and the training and exercises programme), the Copernicus Service for Security (CSS), the European Regional Development Fund (ERDF), the Cohesion Fund, the Neighbourhood, Development and International Cooperation Instrument – Global Europe instrument for the Southern and Eastern Neighbourhood and the Instrument for Pre-Accession, the Technical Support Instrument (TSI), the OLAF Union Anti-Fraud Programme (UAFP) and EU4Health.

From the supply side (funding for European innovators who develop and commercialise security solutions), the promotion of the uptake of the results of Cluster 3 research could involve the Innovation Fund and, to a lesser extent, EU actions under the ISF and the BMVI, as well as Health Emergency Preparedness and Response HERA Invest and the European Institute of Innovation and Technology (EIT).

Practical ways in which Cluster 3 will continue to improve and promote synergies include raising Member States' and Associated Countries authorities' and innovators' awareness of the opportunities for funding for uptake in other EU programmes and instruments, and tracking and studying uptake of Cluster 3 projects' results in other EU programmes and instruments; planning actions in other EU funding programmes and instruments to fund innovation in civil security that takes up the results of Cluster 3 research.

Research funded under Cluster 3 will continue to focus exclusively on civilian applications. Coordination with the European Defence Fund (EDF) and the EU Space Programme will be sought to strengthen cross-cluster complementarities also with actions foreseen in particular in Horizon Europe Clusters 2 and 4[4].

**Role of the Justice and Home Affairs (JHA) agencies**

EU JHA agencies and in particular Europol[5], Frontex[6] and eu-LISA[7] take on a particular role in Horizon Europe. They assist the European Commission on relevant research and innovation

[4] To this end, the Commission and Member States have in place a mechanism for strategic planning and coordination of R&D related to the Copernicus Security Services (CSS), which maps current operational services and on-going and planned R&D initiatives, as well as it identifies end-user operational requirements and promotes sharing of information between projects with common interests. The mechanism drives R&D objectives listed in a Strategic Research Agenda (SRA) updated on a yearly basis. Engagement in the CSS-SRA information sharing process is therefore sought, for those projects planning to use Earth Observation and associated services for civil security applications.

[5] https://www.europol.europa.eu/operations-services-and-innovation/grants/requests-for-europol-participation-in-grants-awarded-other-entities

activities and on specific topics that they identify as desirable to be involved after grants have been awarded.

Proposals should foresee that JHA agencies could observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the civil security research community.

EU JHA agencies are, however, not eligible to participate in any proposal preparation phase and should not be contacted and no documentation should be sent by applicants/consortium members before grants have been awarded.

Similarly, if the proposals concern drug-related issues, successful projects are expected to engage with the European Union Drugs Agency (EUDA) during the lifetime of the project, including validating the outcomes.

For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding.

**Implementation**

Proposals under certain topics in this Work Programme should plan their activities opting for the Financial Support to Third Parties (FSTP)[8].



6 https://www.frontex.europa.eu/innovation/eu-research/news-and-events/new-eu-funded-border-security-projects-fv5jMw#:~:text=Horizon%20Europe%20is%20the%20framework,Frontex's%20role%20is%20further%20strengthened

7 ttps://www.eulisa.europa.eu/

8 For more information on FSTP see: https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=25559615

# Calls

## Call - Civil Security for Society 2026

***HORIZON-CL3-2026-01***

### Overview of this call[9]

Proposals are invited against the following Destinations and topic(s):

| Topics | Type of Action | Budgets (EUR million) | Expected EU contribution per project (EUR million)[10] | Indicative number of projects expected to be funded |
|---|---|---|---|---|
| | | 2026 | | |
| Opening: 06 May 2026<br>Deadline(s): 05 Nov 2026 | | | | |
| Destination - Better protect the EU and its citizens against Crime and Terrorism | | | | |
| HORIZON-CL3-2026-01-FCT-01: Improving capabilities of law enforcement to counter climate-related challenges | RIA | 8.00 | Around 4.00 | 2 |
| HORIZON-CL3-2026-01-FCT-02: Open topic on preventing and countering the misuse of emerging technologies for criminal purposes, including issues related to lawful access to data | RIA | 9.00 | Around 4.50 | 2 |
| HORIZON-CL3-2026-01-FCT-03: Missing persons: prevention and investigation | IA | 5.00 | Around 5.00 | 1 |
| HORIZON-CL3-2026-01-FCT-04: Crime prevention approaches, online and off-line, tackling the nexus between addictions and crime | RIA | 6.00 | Around 3.00 | 2 |

[9] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2026 and 2027.

[10] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | | | | |
|---|---|---|---|---|
| HORIZON-CL3-2026-01-FCT-05: Enhancing the security of citizens against terrorism and lone-actor violence in confined spaces such as schools | IA | 9.67 | Around 4.835 | 2 |
| HORIZON-CL3-2026-01-FCT-06: Prevention and mitigation of misuse of synthetic biology for bioterrorism purposes | RIA | 3.00 | Around 3.00 | 1 |
| Destination - Effective management of EU external borders | | | | |
| HORIZON-CL3-2026-01-BM-01: Advanced border surveillance and situational awareness | IA | 12.00 | Around 6.00 | 2 |
| HORIZON-CL3-2026-01-BM-02: Accessible and available travel facilitation | IA | 8.00 | Around 4.00 | 2 |
| HORIZON-CL3-2026-01-BM-03: Reliability of age assessment methods in the context of security and border management | CSA | 1.33 | Around 1.33 | 1 |
| Destination - Resilient Infrastructure | | | | |
| HORIZON-CL3-2026-01-INFRA-01: Tools and processes to support stress tests of critical infrastructure | IA | 9.67 | Around 4.835 | 2 |
| HORIZON-CL3-2026-01-INFRA-02: Security challenges of the green transition in urban und peri urban areas | RIA | 4.00 | Around 4.00 | 1 |
| HORIZON-CL3-2026-01-INFRA-03: Targeted innovative capabilities for the resilience of critical entities to natural and human-induced disasters, including hybrid scenarios | IA | 9.00 | Around 4.50 | 2 |
| Destination - Disaster-Resilient Society for Europe | | | | |
| HORIZON-CL3-2026-01-DRS-01: Designing new ways of risk awareness and enhanced disaster preparedness | RIA | 6.00 | Around 3.00 | 2 |
| HORIZON-CL3-2026-01-DRS-02: Multi-hazard approach and cumulative / cascading impacts | IA | 8.00 | Around 4.00 | 2 |
| HORIZON-CL3-2026-01-DRS-03: Development of innovative tools, processes, | IA | 8.00 | Around 4.00 | 2 |

| | | | | |
|---|---|---|---|---|
| equipment and technologies through responses to disasters and emergencies for search and rescue in hazardous conditions | | | | |
| HORIZON-CL3-2026-01-DRS-04: Open topic on driving innovation uptake of disaster risk solutions | IA | 6.00 | Around 3.00 | 2 |
| HORIZON-CL3-2026-01-DRS-05: Climate security and civil preparedness – new ways to develop pre- and post-crisis climate-change related scenarios for a more resilient Europe | IA | 4.50 | Around 4.50 | 1 |
| Destination - Strengthened Security Research and Innovation | | | | |
| HORIZON-CL3-2026-01-SSRI-01: Open topic on supporting disruptive technological innovations for civil security | RIA | 3.00 | Around 1.50 | 2 |
| HORIZON-CL3-2026-01-SSRI-02: Demand-led innovation in security | PCP | 5.83 | Around 5.83 | 1 |
| HORIZON-CL3-2026-01-SSRI-03: Public procurement of innovation for security | PPI | 2.00 | Around 2.00 | 1 |
| HORIZON-CL3-2026-01-SSRI-04: Development of ecosystem and next-generation capabilities for a secured European Critical Communication System in civil security | IA | 3.00 | Around 3.00 | 1 |
| Overall indicative budget | | 131.00 | | |

| **General conditions relating to this call** | |
|---|---|
| *Admissibility conditions* | The conditions are described in General Annex A. |
| *Eligibility conditions* | The conditions are described in General Annex B. |
| *Financial and operational capacity and exclusion* | The criteria are described in General Annex C. |
| *Award criteria* | The criteria are described in General Annex D. |

| | |
|---|---|
| *Documents* | The documents are described in General Annex E. |
| *Procedure* | The procedure is described in General Annex F. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. |

**Call - Civil Security for Society 2027**

***HORIZON-CL3-2027-01***

**Overview of this call[11]**

Proposals are invited against the following Destinations and topic(s):

| Topics | Type of Action | Budgets (EUR million) | Expected EU contribution per project (EUR million)[12] | Indicative number of projects expected to be funded |
|---|---|---|---|---|
| | | 2027 | | |
| Opening: 05 May 2027<br>Deadline(s): 04 Nov 2027 | | | | |
| Destination - Better protect the EU and its citizens against Crime and Terrorism | | | | |
| HORIZON-CL3-2027-01-FCT-01: Online harms detection and investigation tools using a short development cycle model | IA | 7.83 | Around 7.833 | 1 |
| HORIZON-CL3-2027-01-FCT-02: Community policing in diverse societies in Europe | IA | 6.00 | Around 3.00 | 2 |
| HORIZON-CL3-2027-01-FCT-03: Open topic | RIA | 6.00 | Around | 2 |

[11] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2026 and 2027.

[12] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | | | | |
|---|---|---|---|---|
| on enhanced prevention, detection and deterrence of societal issues related to various forms of crime | | | 3.00 | |
| HORIZON-CL3-2027-01-FCT-04: Open topic on increasing security of citizens against terrorism, including in public spaces | IA | 9.00 | Around 4.50 | 2 |
| HORIZON-CL3-2027-01-FCT-05: Effective and evidence-based responses to the increased availability and use of synthetic drugs and stimulants in Europe | IA | 8.00 | Around 4.00 | 2 |
| Destination - Effective management of EU external borders | | | | |
| HORIZON-CL3-2027-01-BM-01: Open topic on research and innovation for effective management of EU external borders that promotes fundamental rights and EU values | RIA | 8.00 | Around 4.00 | 2 |
| HORIZON-CL3-2027-01-BM-02: Trusted, secure, quality future digital travel credentials | RIA | 8.00 | Around 4.00 | 2 |
| HORIZON-CL3-2027-01-BM-03: Detection and characterisation of threats or illegal/ smuggled goods in cargo | RIA | 14.00 | Around 3.50 | 4 |
| Destination - Resilient Infrastructure | | | | |
| HORIZON-CL3-2027-01-INFRA-01: Enhancing physical protection of critical infrastructures | IA | 12.00 | Around 6.00 | 2 |
| HORIZON-CL3-2027-01-INFRA-02: Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity | IA | 7.67 | Around 3.835 | 2 |
| Destination - Disaster-Resilient Society for Europe | | | | |
| HORIZON-CL3-2027-01-DRS-01: Open Topic on advanced protective gear optimized for CBRN-E (Chemical, Biological, Radiological, Nuclear, Explosives) environments and new generation of smart protective equipment for disaster responders | IA | 7.67 | Around 3.835 | 2 |
| HORIZON-CL3-2027-01-DRS-02: Societal resilience, engagement of the younger | RIA | 6.00 | Around 3.00 | 2 |

| | | | | |
|---|---|---|---|---|
| generations and digital innovation for disaster resilience | | | | |
| HORIZON-CL3-2027-01-DRS-03: Enhancing decision support system for disaster crises: leveraging emerging technologies for improved civil preparedness and crisis management | IA | 9.00 | Around 3.00 | 3 |
| HORIZON-CL3-2027-01-DRS-04: Enhancing preparedness for large-scale cross-border disasters | IA | 8.00 | Around 4.00 | 2 |
| Destination - Strengthened Security Research and Innovation | | | | |
| HORIZON-CL3-2027-01-SSRI-01: Accelerating uptake through open proposals for advanced SME innovation | IA | 4.50 | Around 1.50 | 3 |
| HORIZON-CL3-2027-01-SSRI-02: Open grounds for future pre-commercial procurement of innovative security technologies | CSA | 2.00 | Around 1.00 | 2 |
| HORIZON-CL3-2027-01-SSRI-03: Demand-led innovation in security | PCP | 5.83 | Around 5.83 | 1 |
| Overall indicative budget | | 129.50 | | |

| **General conditions relating to this call** | |
|---|---|
| *Admissibility conditions* | The conditions are described in General Annex A. |
| *Eligibility conditions* | The conditions are described in General Annex B. |
| *Financial and operational capacity and exclusion* | The criteria are described in General Annex C. |
| *Award criteria* | The criteria are described in General Annex D. |
| *Documents* | The documents are described in General Annex E. |
| *Procedure* | The procedure is described in General Annex F. |

| | |
|---|---|
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. |

# Destinations

## Destination - Better protect the EU and its citizens against Crime and Terrorism

As underlined in the Horizon Europe strategic plan 2025-2027, "*this Destination will support the Commission's priorities by addressing new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving the prevention, detection and deterrence of various forms of crime or terrorism/radicalisation through an enhanced understanding of the related societal issues. In doing so, research and innovation projects funded under cluster 3 will contribute to safeguarding, sustaining, and improving the Union's unique quality of life, by improving the Union's ability to prevent, detect, and deter various forms of crime and terrorism, including the different forms of hybrid threats and gender-based violence, in a proportional and human rights-compliant manner. Research under this Destination will contribute to the forthcoming Internal Security Strategy and Counter-Terrorism Agenda*".

This destination will support the implementation of the European Commission political guidelines 2024-2029 for a 'Safer and more secure Europe' as well as of ProtectEU[13] – a European Internal Security Strategy to support Member States and bolster the EU's ability to guarantee security for its citizens, and the Preparedness Union Strategy to support Member States and enhance Europe's capability to prevent and respond to emerging threats. Overall, research under this Cluster should continue to focus on preserving and ensuring citizens' basic right to feel secure. This destination will also support the European Commission efforts towards a new Counter-Terrorism Agenda to address new and emerging threats, and a united approach to security, centred around a new European Critical Communication System to be used by public authorities in charge of security and safety.

To this end, proposals should contribute to the achievement of one or more of the following impacts:

- Modern information analysis for Police Authorities, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Improved forensics and lawful evidence collection, increasing the capabilities to apprehend criminals and terrorists and bring them to the court;
- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime, including cybercrime, and terrorism, such as violent radicalisation, as well as domestic sexual violence, and gender-based violence, with a particular emphasis on protecting populations in a vulnerable situation and victims at increased risk of violence, including those affected by child sexual abuse and juvenile delinquency;
- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);

[13] COM/2025/148 final.

- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;

- More secure cyberspace for citizens, especially children and elderly people, through a robust prevention, detection, and protection from cybercriminal activities.

More specifically, in the rapidly evolving technological and societal landscape, with climate change and environmental aspects increasingly seen as security issues, and with growing threats to citizens in a vulnerable situation, various forthcoming challenges that European society faces deserve dedicated research and innovation actions in the scope of this Destination. Some of them are:

- challenges regarding prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues, such as

    - tackling the nexus between disinformation, hate speech and radicalisation, countering gender-based violence, or fighting violence-as-a-service.

- challenges related to counterterrorism, protection of public spaces, such as

    - improving detection of remote explosives and explosives in closed spaces and urban environments, or

    - use and countering of unmanned systems, including neutralisation of commercial drone attacks.

Research and innovation funded under this Destination will contribute to policy objectives such as those of the:

- Police cooperation package[14] (information exchange[15], automated data exchange for police cooperation - "Prüm II"[16], operational cross-border police cooperation[17]);

- Counter-Terrorism Agenda for the EU[18] (incl. Regulation 2021/784/EU on addressing dissemination of terrorist content online & Directive 2017/541/EU on combating terrorism);

- EU C-UAS Strategy[19] (counter-drone policy);

- EU Strategy to Tackle Organised crime[20];

- EU Strategy on combatting Trafficking in Human Beings[21] (the modified Directive on preventing and combating trafficking in human being and protecting its victims), and the

14 COM/2021/782 final, COM/2021/784 final, ST/8720/2022/INIT.
15 Directive (EU) 2023/977.
16 Regulation (EU) 2024/982.
17 Council Recommendation (EU) 2022/915.
18 COM/2020/795 final.
19 COM/2023/659 final.COM/2023/659 final.
20 COM/2021/170 final.

Proposal to strengthen EU legislation to prevent and fight migrant smuggling[22] (notably its aspect of reinforcing Europol's role in the fight against migrant smuggling and trafficking in human beings);

- EU drugs measures (Strategy[23], Action Plan[24] and Roadmap to fight Drugs Trafficking and Organised Crime[25]);
- EU Action Plan on firearms trafficking (COM(2020) 608 final);
- Roadmap for lawful and effective access to data for law enforcement (COM/2025/349 final);
- EU environmental crime measures[26] (review of the Directive 2008/99/EC on protection of the environment through criminal law);
- EU anti-corruption measures (Communication[27], proposal for a Directive[28]);
- Directive (EU) 2019/713 on non-cash means of payment;
- EU strategy on a more effective fight against child sexual abuse[29] (incl. Proposal for a regulation to prevent and combat child sexual abuse[30]);
- EU Regulation (2022/2371) on serious cross-border threats to health;
- Directive (EU) 2024/1385 on combating violence against women and domestic violence.

This Destination will also support, whenever appropriate and applicable, proposals with:

- a clear strategy on how they will adapt to the fast-evolving environment in the area of fight against crime and terrorism (evolution of related technologies, evolution of criminal modi operandi and business models related to these technologies, etc.);
- the involvement of Police Authorities in their core;
- the involvement of other law enforcement authorities including customs and border guards;
- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);

---

21 COM/2021/171 final; Directive (EU) 2024/1712; COM/2023/755 final.
22 COM/2023/754 final.
23 14178/20.
24 ST/9819/2021/INIT.
25 COM/2023/641 final.
26 Directive (EU) 2024/1203.
27 JOIN(2023) 12 final.
28 COM/2023/234 final.
29 COM/2020/607 final.
30 COM/2022/209 final.

- the active involvement of Small and Medium Enterprises (SMEs);
- a minimum-needed platform, i.e., tools that are modular and can be easily plugged into another platform (in order to avoid platform multiplication);
- tools that are developed and validated against practitioners' needs and requirements;
- tools following existing or new standards for data exchange, including cybersecurity best-practices;
- a robust plan on how they will build on the relevant predecessor projects;
- education and training aspects, especially for Police Authorities and other relevant practitioners, as well as information sharing and citizen awareness raising;
- a clear strategy on the uptake and sustainability of the project results, with special attention to the access at little or no cost to created tools and methodologies by Police Authorities involved in the project;
- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, in coordination with the Community for European Research and Innovation for Security (CERIS)[31].

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2026-01-FCT-01: Improving capabilities of law enforcement to counter climate-related challenges**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. |

[31] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

| | |
|---|---|
| *project* | Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[32] from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [33]. |
| *Security Sensitive* | Some activities resulting from this topic may involve using classified |

[32] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

[33] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Topics* | background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Police Authorities in Europe are equipped with specialised skills and technologies to counter an increase in illegal activities related to the climate change and the emergence of new (opportunistic) criminal patterns;
- Improved understanding by policymakers of the effects of climate change on law enforcement with a view of developing related effective European policies;
- improved knowledge of the impacts of climate change phenomena on social dynamics which can raise demands from public authorities to keep public order, moving beyond traditional perspectives about crime and terrorism.

Scope: Global climate change is a megatrend expected to affect our societies over the next decade. As stated in "Germany: National interdisciplinary climate risk assessment"[34], "We are already living in the climate crisis. This brings substantial security risks at global and national levels. (...) Anyone thinking about security needs to think about climate as well".

Climate change will affect European law enforcement in various ways [35, 36]. Notably, it is likely to create new opportunities and resources for organised crime, challenging current security frameworks. One of the expected outcomes of climate change will be the emergence of scarcity markets. Links between resource scarcity propelled by climate change and the crime opportunities for organised crime groups need to be further analysed. Criminal networks will aim to dominate the scarcity markets, increasing their role in the distribution of essential goods and services such as food and water. In addition, criminal networks will facilitate the movement of migrants, including women and children, escaping conflict and the effects of climate change; increased flux of migration due to extreme weather conditions may raise opportunities for human trafficking and exploitation. Furthermore, the decline in biodiversity will translate into more animal species under threat of extinction targeted by wildlife traffickers. In this landscape, the adoption of new technologies will bolster criminal organizations of various kinds. Examples of such crimes, illegal activities, threats and harms connected to climate change include: environmental crimes contributing to climate change (illegal mining and extraction, illegal use of underwater sources and streams, illegal deforestation, illegal waste management), wildlife trafficking and poaching, fraud and

34 https://metis.unibw.de/assets/pdf/National_Interdisciplinary_Climate_Risk_Assessment.pdf

35 A.Matczak, S.I. Bergh, A review of the (potential) implications of climate change for policing practice worldwide. Policing: A Journal of Policy and Practice, Vol. 17, 2023, https://doi.org/10.1093/police/paad062

36 P. Schwartzstein (2024), Climate Change & Crime: A big, bad, largely overlooked nexus. The Council on Strategic Risks. https://councilonstrategicrisks.org/2024/10/17/climate-change-crime-a-big-bad-largely-overlooked-nexus/

financial crimes (greenwashing, carbon credit fraud, misuse of climate funds), exploiting climate change-related disasters (water theft, looting after disasters, land grabbing), or social tensions (new forms of radicalisation and terrorism, increased displacement and migration challenging public order and disproportionately affecting groups in a vulnerable situation).

New approaches centred around crime and climate change, including crime activities' association with and amplification by climate change, present unique challenges that require thorough investigation and analysis. Recognizing these emerging trends is vital for formulating effective plans and policies, and equipping law enforcement with specialized skills, technology (including forensics) and training necessary to tackle these challenges in an increasingly volatile world.

In this topic, apart from the mandatory participation of Police Authorities in the consortia, active involvement of other security practitioners, such as civil security services, Border Guard or Customs Authorities, is encouraged if relevant. Technological and societal angles should be addressed in a balanced way.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

This topic requires the effective contribution of Social Sciences and Humanities (SSH) disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related research activities. Research in this area could be strengthened by considering the gender-specific dimensions of vulnerabilities and needs when relevant.

**HORIZON-CL3-2026-01-FCT-02: Open topic on preventing and countering the misuse of emerging technologies for criminal purposes, including issues related to lawful access to data**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |

| | |
|---|---|
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[37] from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>Subject to restrictions for the protection of European communication networks.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [38]. |
| *Security Sensitive* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and |

[37] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

[38] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Topics* | SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- Police Authorities in Europe are empowered with modern, accessible and validated tools, methodologies and training curricula to anticipate and cope with the misuse of new and emerging technologies for criminal purposes, with the aim to facilitate prevention, detection, efficient data access and investigation of criminal offences in a lawful manner and with full respect of fundamental rights, including the right to protection of personal data and to privacy;

- Reinforced interdisciplinary collaboration at the European level through the establishment of partnerships among technologists, policymakers and Police Authorities, resulting in a holistic understanding of the challenges posed by emerging technologies and in sharing of best practices;

- Clear guidelines and frameworks are created, including on procedures and rules, that ensure lawful access to data, balancing the needs of security with respect for privacy and that foster a European approach to the related challenges for the police and the judiciary.

Scope: New and emerging technologies (e.g., new communication technologies, quantum technologies, new biometrics and identification technologies, cloud computing technologies, generative AI etc.) bring many benefits but also pose a number of new challenges for the police and the judiciary. Therefore, there is a strong need to adequately tackle challenges for Police Authorities stemming from all these new and emerging developments as well as to make sure that the lawful access to data keeps track with these evolutions, respecting applicable legislation and fundamental rights such as personal data protection and privacy.

Under the Open topic, proposals are welcome to address new and emerging technologies that are not covered by the other projects of the previous Horizon Europe Calls Fighting Crime and Terrorism, as well as of the current Call Fighting Crime and Terrorism 2026-2027. Proposals should emphasize adaptive methodologies and frameworks that can evolve in response to new threats and challenges, empowering Police Authorities to act effectively while ensuring adherence to legal standards regarding data access. Thus, research activities proposed within this topic should, in a balanced way, 1) develop modern tools, methodologies and training material for police to tackle the problem of misuse for criminal purposes of the new and emerging technologies under consideration, and 2) address issues related to lawful access to data in this context.

In this topic the integration of the gender and intersectional dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

The proposals funded under this topic that concern issues which are within the mandate of Europol[39] are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2026-01-FCT-03: Missing persons: prevention and investigation**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 5.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[40] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the |

[39] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794 (Annex I).

[40] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| | template provided in the submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [41]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved skills, tools and training curricula for Police Authorities in Europe and Civil Society Organisations (or Non-Governmental Organisations) to work with at-risk groups to prevent persons from going missing. Those improved skills, tools and training curricula are to take into account European multicultural dimension, as well as legal and ethical rules of operation;

- Enhanced investigation tools and methodologies for Police Authorities in Europe to tackle cold cases in the context of missing persons, based on modern (forensic) technologies and criminology;

[41] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Modern training curricula for Police Authorities, their improved cross-border cooperation and enhanced tools and methodologies to tackle new cases of missing persons;

- Enriched European common approaches applied by Police Authorities in Europe to fight the issue of missing persons relying on the synergy of technology, the latest socio-psychological knowledge learned from cases, as well as field experience of Police Authorities and entities dealing with victims, while fully respecting fundamental rights such as privacy, protection of personal data and anonymity of victims.

Scope: The issue of missing persons is a multifaceted challenge that encompasses diverse categories and is influenced by various factors. People may go missing under a variety of circumstances, such as voluntary disappearances, abductions, cases related to mental health crises, or because of conflict, migration, geopolitical instability, natural disasters. Groups in a vulnerable situation - notably children, victims of trafficking and exploitation, persons with disabilities and persons suffering from cognitive impairments - face an even greater risk of going missing, often under distressing and dangerous conditions. Tackling this issue requires a coordinated response from multiple stakeholders, from Police Authorities via Civil Society Organisations (CSOs) or Non-Governmental Organisations (NGOs) to the involvement of the overall society.

In an era of rapid technological advancement and societal developments, there is a pressing need to improve current European approaches to fight the issue of missing persons (prevention and/or investigation of cold and new cases) using innovative societal and technological solutions. To this end, modernised skills, training curricula and methodologies for Police Authorities, CSOs and NGOs to work with people in a vulnerable situation and children are needed, such as effective awareness raising campaigns, which should be accessible to persons with disabilities, that take into account European multicultural dimension. When it comes to investigation, Police Authorities need efficient tools that benefit from new and emerging technologies to solve cold cases while combining modern forensic science (including biometrics and digital forensics) and criminology, e.g., modern tools for using an old DNA, or accurate facial ageing, among others. When multiple practitioners are involved in exchanging sensitive data, data sharing tools in a privacy-preserving manner should be considered. Furthermore, for new cases of missing persons, apart from an improved cross-border cooperation, Police Authorities also need, on the one hand, a modernised training to face such situations more efficiently, improving the dialogues and interactions with families, taking into account a gender sensitive and intersectional approach when relevant, and on the other hand, modern technologies and forensic tools for, for example, fast and reliable cross-matching of DNA samples between new and cold cases.

If a proposal concerns forensics, its consortium should involve forensic institutes as well. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project, including validating the

outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2026-01-FCT-04: Crime prevention approaches, online and off-line, tackling the nexus between addictions and crime**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[42] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology* | Activities are expected to achieve TRL 5 by the end of the project – see |

[42] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| *Readiness Level* | General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [43]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved understanding of links between addictions and crime, including drivers of criminality;
- Innovative and effective solutions, including training curricula, for Police Authorities in Europe and relevant Civil Society Organisations (or Non-Governmental Organisations) to prevent addictions and related crimes, with a special attention to young people at risk;
- Evidence-based support to modernising European criminal justice system's approach when dealing with addiction-related offenses;
- Novel approaches of collaboration between different stakeholders, primarily Police Authorities in Europe and Civil Society Organisations (or Non-Governmental Organisations), to increase communities' addiction resilience, security and safety.

Scope: A close and complex relationship exists between addictions, such as gambling, drug or alcohol use, and crime (e.g., criminals are often under the influence of drugs while committing crimes, gamblers or drug users commit crimes to pay for their debts or drugs). In this topic, successful proposals are expected to analyse the specific nexus between addictions and crime, with the aim of developing related modern methodologies and tools for prevention of not only addictions but also crimes related to them, both offline and online, while

[43] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

respecting the fundamental rights of the communities concerned and using of non-stigmatising language. Novel approaches of collaboration between different community stakeholders, from Police Authorities, civil society, national and local entities, private actors, trained psychologists, are expected to be developed as well, with the aim of increasing communities' addiction resilience, security and safety. An emphasis of the work should be on young people at risk, the criminal justice system, drivers of criminality and pathways from committing a petty crime because of addiction to progressively getting involved in organised crime. Activities proposed within this topic should address the issue from various angles, combining both social research with technological development and applications in a logical manner.

Therefore, this topic requires the effective contribution of Social Sciences and Humanities (SSH) disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related research activities. Also, incorporating a gender-sensitive approach will allow to better understand the relationships between addiction, crime, and gender, leading to more effective interventions that address the specific needs of men, women, and marginalized groups.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Furthermore, proposals funded under this topic are expected to provide ideas on how they would engage with the European Union Drugs Agency (EUDA) during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2026-01-FCT-05: Enhancing the security of citizens against terrorism and lone-actor violence in confined spaces such as schools**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.835 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.67 million. |

| | |
|---|---|
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[44] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [45]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

[44] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

[45] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Increased understanding of policymakers and relevant security practitioners of the phenomenon of terrorism and lone-actor violence towards citizens in confined places such as schools, in the European context;
- Terrorist and lone-actor attacks to citizens in confined places such as schools, are prevented in Europe by, e.g., detecting and tackling early signs of isolation and radicalisation, as well as the promotion of a secure and inclusive environment;
- European schools and other confined places, e.g., places of worship, public administration or other buildings accessible to the public, are provided with state-of-the-art means of ensuring their security;
- Cooperation between Police Authorities in Europe and relevant staff (in schools, public administration, etc.) is improved.

Scope: Citizens in European schools and other confined spaces (e.g., places of worship, public administration and other buildings accessible to the public) increasingly face various forms of terrorism and lone-actor violence. This topic aims at providing such places with solutions for ensuring civil security (of pupils, school staff, administrative workers, citizens at large) via exploring various societal and technological means of preventing such threats, with full respect of fundamental rights, such as rights to privacy and the protection of personal data. Based on a thorough analysis of the phenomenon under consideration in the European context, proposals should look into methodologies of catching and tackling early signs of terrorist threats, isolation and radicalisation, taking into account the social and cultural factors that may influence an individual's vulnerability to radicalisation, such as gender roles and stereotypes. Proposals should also consider how these factors may impact the effectiveness of prevention programmes and of addressing them by, e.g., creating appropriate programmes, including by modernising approaches for prevention of terrorist and lone actor attacks. Means for raising awareness (possibly training) of the relevant staff (school staff, employees in public administration, etc., in function of the building under consideration) regarding existing risks and for keeping them up to date on security matters should be tackled and designed to be inclusive and effective for diverse groups. Ways of improving cooperation between the relevant staff and Police Authorities in this context should be analysed too. Proposed solutions should be affordable to public schools and other structures accessible to the public that are usually more limited in funding. Proposals are invited from consortia involving Police Authorities and other relevant security practitioners, Civil Society Organisations, Non-Governmental Organisations, and the appropriate balance of IT specialists, psychologists, sociologists, etc. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project’s mid-term outcomes, performed by the practitioners involved in the project. Activities proposed within this topic should address the issue from various angles,

combining both social research with technological development and applications in a logical manner.

Therefore, this topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related research activities.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on outcomes developed by EU-funded projects, such as the ones under HORIZON-CL3-2024-FCT-01-04 and HORIZON-CL2-2025-01-DEMOCRACY-05, and not duplicate previous research. If the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2026-01-FCT-06: Prevention and mitigation of misuse of synthetic biology for bioterrorism purposes**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of* | The rules are described in General Annex G. The following exceptions apply: |

| | |
|---|---|
| *the Grant Agreements* | The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [46]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- Increased understanding of European policy makers, research community, biotech companies, and relevant security practitioners of the threat of bioterrorism and of synthetic biology, including a thorough lawful analysis of what needs to be monitored in this context, what needs to be regulated and how;
- Awareness raised within the related scientific community how research in synthetic biology can be used for malicious purposes.

Scope: The rising threat of bioterrorism is driven by recent scientific advancements, notably by growing accessibility of synthetic biology, genetic engineering, related commercial services and public databases, which in turn enhance their obtainability to non-state actors and individuals with malicious intentions. The proliferation of do-it-yourself biohacking and community laboratories, including gene editing and sequencing technology, dropping costs of equipment and increased simplicity of use may inadvertently facilitate knowledge and skills dissemination about biological threats and open new pathways for bioterrorism. Challenges in detection, particularly the lengthy incubation periods of biological agents, underscore the urgent need for improved identification technologies to allow for timely intervention and reduce potential mass casualties, considering both characterization through advanced tools by expert labs and simple deployable methods. Given that properly weaponized biological agents can be more lethal than nuclear weapons, their cross-border implications warrant focused attention. Recent incidents involving biotoxins across various European countries illustrate the feasibility of biological attacks. The increasing weaponisation of drones highlights an alarming trend that could extend to biological agents, further complicating threat landscapes.

[46] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

The potential economic and social consequences of biological attacks necessitate robust prevention and preparedness measures to mitigate overwhelming impacts on healthcare systems and society at large.

Proposals are expected to address, in a lawful manner, the emerging threats of bioterrorism in Europe, particularly in the context of synthetic biology. Recognising bioterrorism as a low-probability but high-impact event, consortia should review current and future risks, flag areas requiring reinforced monitoring, as well as identify missing regulatory frameworks necessary for ensuring public security and safety. Furthermore, proposals should bring together diverse consortia to enhance our understanding, prevention, preparedness, and response to bioterrorism and create a comprehensive approach to this pressing issue.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2027-01-FCT-01: Online harms detection and investigation tools using a short development cycle model**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 7.833 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 7.83 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply: |

| | |
|---|---|
| | The following additional eligibility conditions apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[47] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [48]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and |

[47] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

[48] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| | SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- Police Authorities in Europe benefit from a rapid deployment of targeted detection and investigation tools and related training materials, specifically tailored to counter current, foreseeable and emerging online harms at the outset of each development cycle;
- Police Authorities in Europe are provided with a flexible framework for adaptation via creation of a modular toolset that allows for the incorporation of new functionalities and updates based on the latest trends and threats in online harms;
- Enhanced European stakeholder collaboration through facilitation of partnerships among researchers, policymakers, and Police Authorities in Europe to ensure that tools are not only effective but also user-friendly, legally and ethically sound.

Scope: As the digital landscape continues to evolve, so too do the myriads of online harms that threaten citizens' security and well-being. To address these challenges, we invite proposals for the development of detection and investigation tools that employ short development cycle models. This approach emphasizes agility and responsiveness, ensuring that tools can quickly adapt to emerging online threats, such as identity theft, disinformation, deepfakes, spoofing, phishing, digital violence, or, e.g., tools for an early detection as well as real-time monitoring and risk assessment that can identify potential fraudulent sales ("online payment fraud") before they occur.

This topic welcomes innovative ideas focused on creating efficient detection and investigation tools to combat varying forms of online harms, which should be selected at the beginning of every new development cycle, in agreement with all stakeholders involved in the consortia, especially including concrete needs of Police Authorities. The emphasis on short development cycles allows proposals to remain dynamic, responsive to the fast-paced nature of online threats, and capable of addressing both established issues and new challenges as they arise. Proposals should focus on the iterative process of tool development, integrating feedback from Police Authorities to ensure continuous improvement and relevance in combating online harms. Ultimately, the goal is to foster a proactive and effective response to safeguarding online spaces for all users, regardless of their gender identity or expression.

Proposals are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project. Furthermore, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the

project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination. The project should have a minimum estimated duration of 48 months.

**HORIZON-CL3-2027-01-FCT-02: Community policing in diverse societies in Europe**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[49] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |

[49] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [50]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- New tools, skills and methodologies for Police Authorities in Europe to deal efficiently with diverse communities as well as with diversity among police personnel are identified, developed and disseminated throughout Europe, leading to, among others, an increased trust to Police Authorities in general;
- Modern and effective training curricula for Police Authorities in Europe are developed on community policing in diverse societies, including post-conflict zones, and addressing the needs of individuals from various social, ethnic and religious backgrounds, as well as marginalized groups such as migrants, LGBTIQ people, persons with disabilities, or returnees from war.

Scope: This topic addresses challenges of community policing in increasingly diverse and sometimes also fragile societies, including the integration of returnees from conflict zones, migrants, as well as marginalized communities including LGBTIQ individuals and various ethnic and religious groups.

Encompassing a post-conflict dimension too, particularly in the context of Ukraine, this topic aims to foster inclusive community policing practices that can adapt to the complexities of

[50] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

diverse societal dynamics. Proposals should explore innovative and inclusive approaches in police education, training and management that go beyond traditional models, resulting in an effective engagement with a diversifying society. Proposals should also seek to identify and develop effective practices and training programs that encourage a deeper understanding of diversity among police personnel and integrate a gender-sensitive and intersectional approach when relevant. In addition, proposals should assess how effective cooperation with Civil Society Organizations (or Non-Governmental Organisations) - representing various communities - can enhance reporting mechanisms, reduce hate crimes, and strengthen trust and cooperation between the police and the population. By improving police-citizen relations across diverse European contexts, the proposals should aim to contribute to enhanced security and social stability in Europe. Proposals' findings should generate valuable insights applicable to varied policing environments, ultimately informing police forces across Europe about non-violent conflict resolution and constructive engagement strategies. Through collaborative research and training, proposals should equip Police Authorities with the tools, skills and methodologies necessary to effectively serve and engage with diverse communities, foster social cohesion, and build trust throughout Europe.

Activities proposed within this topic should address the issue from various angles, combining social sciences with technological development and applications in a logical manner.

Therefore, this topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related research activities.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Furthermore, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2027-01-FCT-03: Open topic on enhanced prevention, detection and deterrence of societal issues related to various forms of crime**

| **Call: Civil Security for Society 2027** |
| --- |
| **Specific conditions** |

| | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[51] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [52]. |

[51] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

[52] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:

| | |
|---|---|
| | Beneficiaries must provide financial support to third parties. The support to third parties can only be provided in the form of grants. The maximum amount to be granted to each third party is EUR 60 000 to support effective collaboration and/or coordination with additional relevant national Police Authorities and/or CSOs/NGOs from EU Member States or Associated Countries. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved, modern, uniform and validated tools, skills or methodologies as well as innovative training curricula are available for security practitioners (Police Authorities in Europe, Non-Governmental Organisations, Civil Society Organisations) to prevent, detect and deter criminal or terrorist offences under consideration, taking into account all applicable legislation and fundamental rights;
- Enhanced understanding of the cultural and societal aspects of crime or terrorism/radicalisation offences under consideration as well as on the key challenges related to combating them;
- Evidence-based support is available to policymakers on shaping and tuning of regulation related to crime or terrorism/radicalisation offences under consideration;
- Enhanced perception by citizens that Europe is an area of freedom, justice, security and respect of privacy and human rights, thanks to, e.g., innovative awareness-raising campaigns explaining to citizens the key and evolving mechanisms of crime or terrorism/radicalisation offences under consideration, and how to protect against them.

Scope: Under the Open Topic, proposals are welcome to address both existing and upcoming challenges in fighting crimes that are deeply rooted in cultural and/or societal factors that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023-2024 and Fighting Crime and Terrorism 2025 and Fighting Crime and Terrorism 2026-2027.

Adapted to the nature, scope and type of proposed activities, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Proposals should also delineate the plans to develop possible future uptake and upscaling at national and EU level for possible next steps after the research project completion. If applicable, research proposals should consider building on or complementing

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

previous research, including but not limited to, research stemming from Horizon Framework Programmes, such as those funded under HORIZON-CL2 calls.

The proposals funded under this topic that concern issues which are within the mandate of Europol[53] are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. If the funded proposal concerns radicalisation, the consortium is encouraged to liaise with the EU Knowledge Hub on prevention of radicalisation with the aim of facilitating the streamlining of their priorities and the dissemination of their results.

In this topic the integration of the gender and intersectional dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should plan their activities opting for the Financial Support to Third Parties in order to provide financial support to practitioners (Police Authorities and/or Non-Governmental Organisations/Civil Society Organisations) for expanding the proposed work in terms of additional user groups, complementary assessments, technology- or methodology-testing activities. From 5% up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties. Proposals must clearly describe the objectives and the expected results to be obtained, including the elements listed in the application template. Proposals are also expected to describe the methods and processes relevant to comply with the general eligibility conditions for financial support to third parties set out in General Annex B and to demonstrate effectiveness (impact).

To ensure the active involvement of and timely feedback from relevant security practitioners, i.e., Police Authorities and Non-Governmental Organisations / Civil Society Organisations, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Activities proposed within this topic should address, in a balanced way, both technological and societal dimensions of the issue under consideration. This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

**HORIZON-CL3-2027-01-FCT-04: Open topic on increasing security of citizens against terrorism, including in public spaces**

**Call: Civil Security for Society 2027**

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794 (Annex I).

| **Specific conditions** | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility conditions apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[54] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5. |

[54] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| | Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [55]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Enhanced ability of Police Authorities in Europe and other relevant security practitioners to identify and prevent emergent challenges in the terrorism-related issue under consideration;
- Harmonised and modern tools as well as procedures are available for Police Authorities in Europe and other relevant security practitioners to counter the terrorism-related problem under consideration, in full compliance with applicable legislation on protection of personal data and protection of fundamental rights;
- Improved cooperation between Police Authorities in Europe and other relevant security practitioners, as well as with international actors, in tackling the problem in question;
- Training curricula are available for Police Authorities in Europe and other relevant security practitioners for an improved countering of the terrorism-related problem under consideration.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for increasing security of European citizens against terrorism, including in public spaces, that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023-2024, Fighting Crime and Terrorism 2025 and Fighting Crime and Terrorism 2026-2027.

Adapted to the nature, scope and type of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. In this topic the integration of the gender dimension (sex and gender

[55] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should also delineate the plans to develop possible future uptake and upscaling at national and EU level for possible next steps after the research project. Research proposals should consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. The proposals funded under this topic that concern issues which are within the mandate of Europol[56] are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**HORIZON-CL3-2027-01-FCT-05: Effective and evidence-based responses to the increased availability and use of synthetic drugs and stimulants in Europe**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[57] and at least 2 Civil Society Organisations (or Non- |

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794 (Annex I).

[57] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

| | |
|---|---|
| | Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [58]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- Evidence base is improved for effective prevention, treatment and harm reduction of synthetic drugs and stimulants in Europe;
- Relevant European security practitioners, notably Police Authorities, Civil Society Organisations and Non-Governmental Organisations, are equipped with skills, tools and technology aimed at reducing the violence and offences associated with use and

[58] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

marketing of these substances, as well as at combatting drug trafficking from its origin to destination (i.e., through the entire supply chain);

- Increased understanding of relevant European security practitioners and policymakers regarding the influence of external drivers of change of societal, technological, legal, economic and ethical nature to the availability and use of different types of synthetic drugs and drug markets.

Scope: This topic asks for proposals that seek to develop effective and evidence-based responses to the growing prevalence of synthetic drugs and stimulants, such as cocaine and crack cocaine, within the EU. As these substances increasingly influence the drug landscape, the urgent need for enhanced understanding and strategies in their prevention, treatment, and harm reduction has never been clearer. Amongst other, there is also a lack of pharmacological data for the emerging drugs, needed to do proper risk assessments and interventions of these drugs in Europe. Key focus areas include:

- Evidence-based approaches, strengthening the evidence base to inform effective prevention strategies, treatment modalities, and harm reduction practices targeted at synthetic drugs and stimulants. This includes identifying best practices in current interventions and evaluating their efficacy.

- Reducing violence and offending exploring strategies to mitigate the violence and criminal behaviour associated with the use and marketing of synthetic drugs. This involves understanding the socio-economic and cultural factors, including the gender, age, or other social factors, that contribute to these phenomena and proposing targeted interventions.

- Improving technologies and tools to combat drug trafficking from its origin to destination (i.e., through the entire supply chain).

- External drivers of change, analysing the impact of geopolitical situations, legal frameworks, and societal factors on the availability and consumption of various drugs, and addressing how international crises affect organised crime and drug markets in the EU. This includes investigating the repercussions of global developments on local drug dynamics and identifying adaptive response strategies.

In light of the underdeveloped evidence base surrounding synthetic drugs, proposals should aim to foster collaboration among researchers, policymakers, and security practitioners to create a comprehensive and effective response to this pressing issue in Europe, previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

Activities proposed within this topic should address, in a balanced way, both technological and societal dimensions of the issue under consideration. The proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, the proposals funded under this topic are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

**Destination - Effective management of EU external borders**

Proposals submitted under this Destination should contribute to the expected impact of the Horizon Europe strategic plan 2025-2027: "facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts".

This Destination will support the implementation of the European Commission Political Guidelines 2024-2029, with research and innovation for future border management contributing to resilience and competitiveness. This includes investing in the update and development of future European digital and integrated border management that respects and promotes EU values. This will contribute to equip European border, coast guards and customs authorities with the future European state-of-the-art solutions, as well as to the preparedness and capabilities to manage future challenges across the EU external borders, including potential instrumentalisation of migration, hybrid attacks, migrant smuggling, and trafficking linked to transnational terrorism and/or organised crime.

Research and innovation under this Destination will focus on preserving and securing the basic right to feel secure and on protecting and promoting fundamental rights as a priority for both European citizens and third country nationals. It will do so by funding projects which will study, develop and test possible future solutions that both strengthen, and make safer, European borders.

Projects funded under this Destination will promote technological and social research and innovation and further explore and develop solutions that enhance the technological sovereignty of European authorities, in the areas of border management, customs and supply chain security, and civilian aviation and maritime security.

To this end, proposals should contribute to the achievement of one or more of the following impacts:

- explore and develop future capabilities for European users in the areas of border management, customs and supply chain security, and civilian maritime security, in particular in the capability areas of:
    - border surveillance;
    - facilitating travel and legitimate trade;
    - assessing and managing risk;
    - strengthening the Schengen area without introducing internal border controls;
    - maritime, aviation, land transport, cargo and customs security;
    - supply chain resilience;
    - detecting and identifying threats;

- interoperability and cybersecurity of EU information systems and equipment;
- safeguarding and promoting fundamental rights in the context of border management.

Research and innovation funded under this Destination will contribute to policy objectives such as:

- the Multiannual Strategic Policy for European Integrated Border Management[59];
- the implementation of the Capability Roadmap of the European Border and Coast Guard[60] and its updates;
- the proposals to strengthen EU legislation to prevent and fight against migrant smuggling[61];
- the proposals on digitalisation of travel documents and facilitation of travel[62];
- the new European Internal Security Strategy[63];
- the new Counter-Terrorism Agenda;
- the European Preparedness Union Strategy[64];
- the EU Port Strategy;
- the civil security aspects of the updated EU Maritime Security Strategy[65] and of the European Ocean Pact;
- the Copernicus service for Security[66] improving crisis prevention, preparedness and response in four key areas: Border surveillance; Maritime surveillance; Support to EU External and Security Actions, R&D for Earth Observation Security;
- the EU Cable Security Action Plan[67];
- the new European action plans against drug trafficking and against weapons trafficking;
- the proposals for EU Customs reform[68], including the proposed EU Customs Authority and Data Hub;

59 COM (2023) 146 final.
60 FRONTEX MB Decision 16/2024.
61 COM/2023/754 final; COM/2023/755 final.
62 COM (2021) 277 final; COM (2024) 670 final.
63 COM/2025/148 final.
64 JOIN(2025), 130 final.
65 JOIN/2023/8 final.
66 Regulation (EU) 2021/696
67 JOIN(2025) 9 final
68 COM (2023) 257 final; COM (2023) 258 final – 2023/0156(COD); COM (2023) 259 final – 2023/0157(NLE); COM (2023) 262 final – 2023/0158(CNS).

- the security aspects of the Comprehensive EU toolbox for safe and sustainable e-commerce[69];
- the security aspects of the Competitiveness Compass for the EU[70].

Research and innovation will contribute to sustain and improve capabilities to cope with potential future critical situations or emerging challenges regarding both the flow of people and the flow of goods across external EU borders. These capabilities may include but not limit to:

- monitoring, preparedness and reaction in border management tasks, managing irregular or illegal activities involving people or goods across external borders of the EU;
- safeguarding and promoting fundamental rights and EU values, and ensuring legal compliance, in efficient border management;
- efficiency, performance, environmental impact and reaction in border management tasks in all geographical and meteorological conditions;
- integrated and continuous border surveillance, situational awareness and analysis support;
- safety, user experience and performance of practitioners' staff in border management;
- security, privacy and usability of identity and (travel) documents and credentials;
- facilitating travel of bona fide passengers across external borders of the EU;
- prevention, detection and disruption of trafficking of dangerous, illicit and illegal goods and materials through external borders of the EU and the supply chain.

Furthermore, research and innovation under this Destination will contribute to:

- safeguard the technological sovereignty of the EU in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base;
- lower the environmental impact and footprint of border, customs and supply chain security tasks, through innovative solutions and methods;
- integrate and improve safety and cybersecurity of EU information systems, of innovative equipment, and of information and data in these areas, especially during their exchange at operational or tactical levels;

69 COM(2025) 37 final.
70 COM(2025) 30 final.

- improve interoperability both among proposed solutions and also with future technological developments in the areas of border management, customs and supply chain security, and civilian maritime and aviation security.

Research projects funded under this Destination should engage with all stakeholders involved, including travellers, migrants, and operators, as relevant.

Projects should align and contribute primarily to the realisation of the Capability Roadmap of the European Border and Coast Guard (EBCG) published by the EBCG Agency (Frontex), especially the Roadmap's mid- and long-term perspectives. The Roadmap provides strategic vision for investments into the development of capabilities and is the result of integrated planning between the Member States and the European Border and Coast Guard Agency. Proposals submitted under this Destination should explain the alignment primarily with the Capability Roadmap and the plans for further uptake of the research outcomes, especially by involved practitioners in line with their national Capability Development Plans.

Frontex will be closely associated with and will assist Member States and the European Commission in drawing up and implementing relevant research and innovation activities. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) may also assist the European Commission on relevant research and innovation activities and specific topics.

At the proposal preparation stage, Frontex and/or eu-LISA will not provide guidance on or otherwise be involved in the preparation of project proposals. However, proposals should consider and anticipate that Frontex and/or eu-LISA may observe pilots and demonstrations during project implementation to facilitate the future uptake of innovations within the border and coast guard community.

To accomplish the objectives of this Destination, additional eligibility conditions have been defined regarding the active involvement of relevant security practitioners or end-users in the research projects' consortia.

Cross-community and cross-authority synergies within civil security can be an asset, for example in relation to combat crime and terrorism (across external borders); Disaster-Resilient Society (regarding natural hazards and disasters); Resilient Infrastructure (regarding threats to infrastructures, coming from across borders).

Proposals submitted under this Destination should demonstrate how they plan to build on relevant predecessor projects; to consider the citizens' and societal perspectives; to include education, training and awareness raising for practitioners and citizens; to measure the achieved TRL.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals. Knowledge and technologies developed by research funded under this Destination may be taken up or tested operationally with co-funding of instruments such as the Integrated Border Management Fund, in its components of

the Border Management and Visa Instrument (BMVI) and Customs Control Equipment Instrument (CCEI), and/or subsequent funding instruments. Member States authorities participating in research projects are encouraged to use those instruments for uptake (piloting, testing, validation, scale-up, transfer, acquire, deploy, etc.) of innovative solutions developed from research, as early as TRL 7.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects.

Successful proposals under this Destination are invited to cooperate with other EU-led or EU-funded initiatives in the relevant domains, such as the Knowledge Networks for Security Research & Innovation funded under Horizon Europe Cluster 3, or other security research and innovation working groups set-up by the Commission or EU Agencies.

Funded projects are encouraged to liaise with the European Commission's Joint Research Centre (JRC), for example with regards to a possibility of testing the relevant research outputs at the JRC Border Security Lab.

Where possible and relevant, synergy-building and clustering initiatives with projects in the same area should be considered, in coordination with the Community for European Research and Innovation (CERIS)[71].

Cluster 3 will further incentivise the use of European Space Programmes' services for border management innovation where relevant and their services and capabilities, including demonstration and validation of new technologies in operational environments.

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2026-01-BM-01: Advanced border surveillance and situational awareness**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |

[71] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

| | |
|---|---|
| *Indicative budget* | The total indicative budget for the topic is EUR 12.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated countries. For these participants, applicants must fill in the table "Eligibility information about practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [72]. |

[72] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved detection, localization, characterization and, when applicable, neutralisation, of unmanned vehicles alone or in swarms, involved in trafficking or smuggling activities across external borders, while complying with legal and ethical guidelines;
- Improved border situational awareness, especially in the context of large-scale movements of people across borders, including from potential instrumentalisation of irregular migration, conflicts, social, economic, environmental and climate stress;
- Better safeguard and promotion of fundamental rights thanks to enhanced situational awareness;
- Reliable, redundant detection and reaction capacities without putting staff and society at risk.

Scope: Capabilities for situational awareness and surveillance of land and sea borders need improvement, in consideration of potential future challenges that may require updated capabilities. These challenges may include potential future large-scale movements of people across external borders, resulting from future attempts to instrumentalisation of irregular migration, but also from conflicts, social, economic, environmental and climate stress in the European neighbourhood; as well as increasing availability and capability of unmanned aerial, surface, and underwater vehicles with increased payload capacity and range that make it easier to transport goods and, possibly, persons, including in connection will illicit or illegal activities such as trafficking of goods and smuggling of people across external EU borders. These challenges will be particularly relevant in regions close to the European neighbourhood.

This may be particularly relevant for unsupervised and difficult-to-control land and sea borders of the Union and the Schengen area.

Research funded under this topic should develop solutions that, through better awareness, improve efficiency and reaction time of detection, search, rescue, and recovery operations near land and sea borders, in diverse geographical and meteorological conditions, taking into account the different and diverse needs. Research funded under this topic can also promote cross-border cooperation at European regional level around innovative border management solutions demonstration testbeds.

Actions funded under this topic should develop solutions that go beyond state-of-the-art in clearly demonstrable ways, including measurable improvements in detection range, accuracy, response time, automation, and system resilience.

Improved border surveillance and situational awareness must better safeguard and promote fundamental rights and EU values, with a particular regard to human rights, using an inclusive approach that addresses diverse needs. Solutions should also provide reliable and redundant capacities, while ensuring the safety of staff, users, and persons who may be victim of illicit activities across external borders.

The EBCG Capability Roadmap recognises that future capabilities that help detect cross-border irregularities and cases requiring Search and Rescue activities are essential. Solutions should be modular and scalable to cater to the regional and challenges specificities.

Compatibility and integration with the European Border Surveillance System (EUROSUR) is essential, and compatibility and/or exploitation of other European information-sharing environments, like the Common Information Sharing Environment (CISE), would be an additional asset.

Proposals should demonstrate that the proposed equipment and technologies contribute to cost reduction and energy efficiency of border surveillance and situational awareness operations.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard (ECBG) and of its Agency (Frontex). This should start from the definition of requirements and the design phase, including alignment with the EBCG Capability Roadmap and on the engagement with the Agency during the project implementation. At the proposal preparation stage, Frontex will not provide guidance on or otherwise be involved in the preparation of project proposals. However, proposals should consider and anticipate that Frontex may observe pilots and demonstrations during project implementation to facilitate the future uptake of innovations within the border and coast guard community.

To ensure active involvement and timely feedback from relevant security practitioners, proposals should include a mid-term deliverable consisting of an assessment of the project's mid-term outcomes, conducted by the practitioners involved in the project.

**HORIZON-CL3-2026-01-BM-02: Accessible and available travel facilitation**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |

| | |
|---|---|
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [73]. |

[73] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved trusted, secure, and easier automated seamless facilitation for travel, border crossing through border crossing points (BCPs), and/or visa procedures with an integrated approach, minimized risk for bias, and accessible for all travellers minimising digital divides;
- Facilitated solutions with same approach adaptable by all European border control staff, in all conditions and border control points (BCPs);
- Reduced workload and improved safety, user experience and performance of practitioners' staff involved in border management.

Scope: Facilitation of travel and border crossings at border crossing points (BCPs) across the external EU borders went, and is further going, through developments thanks to updated procedures and regulatory frameworks and to innovative European technologies. From automated border control (ABC) gates to "no-gate" solutions and "seamless travel", and with systems like the Entry-Exit System (EES), the Electronic Travel and Information Authorisation System (ETIAS), and the development of digital travel credentials and digital identity more in general, Europe has one of the most advanced, secure and facilitated border check systems in the world.

Travel facilitation schemes are still not as fair, inclusive and accessible as they should be. There are several technical exceptions that for example make difficult for families, other groups of people travelling together, people with disabilities and/or reduced mobility, or with relatively lower digital skills, to smoothly use travel and border crossing facilitation solutions. This is a capability gap of travel facilitation systems that has an impact on both a fair accessibility and availability for travellers, and on performance and efficiency of the systems themselves. Travel facilitation systems should ensure both security and easy passenger flow, while remaining accessible to all travellers.

On the other hand, both technical systems and procedures may have differences depending on the context or the BCP of application. This may be a limit for the performance and user experience of European integrated border management, especially in a perspective of a larger help to national members of the European Border and Coast Guard (EBCG) from the Standing Corps of the European Border and Coast Guard Agency (EBCGA).

According to the EBCG Capability Roadmap, legal border crossings should be as swift and simple as possible, while at the same time allowing a smooth crossing of bona fide persons, and of the goods carried with them.

Innovation actions funded under this topic will develop and test solutions for advanced seamless travel and border crossing and/or visa procedures, protecting and promoting fundamental rights, minimising the risk for bias and being accessible for all travellers, with no or minimised limitations depending on age, sex, gender, disability, physical or digital abilities. To minimise potential for discrimination or physical or digital divide regarding travel facilitation schemes, solutions should be inclusive and accessible.

Furthermore, solutions should be tested for use with the same approach by all European border control staff in all conditions and BCPs.

The proposed solutions can include innovative technologies, innovative processes, innovative knowledge and/or a combination thereof. Solutions should include automated decision support systems suggesting to the end-users (border checks operators) which procedure, technology or database can be used without infringing rights of travellers. Solutions should also integrate and, if appropriate, further develop, biometric matching that minimises data shared (for example limiting to matching scores) to improve data protection.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap; and on the engagement with the Agencies during the implementation of the project. At the stage of proposal preparation, Frontex and eu-LISA will not provide any guidance on, or otherwise be involved in the preparation of, project proposals. Proposals should consider and foresee that Frontex and eu-LISA may observe pilots and demonstrations when the project will be implemented, with the aim of facilitating future uptake of innovations for the border, customs and coast guard community.

To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

Depending on the particular scope of the proposal, participation of Customs Authorities is welcome.

**HORIZON-CL3-2026-01-BM-03: Reliability of age assessment methods in the context of security and border management**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.33 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a |

| | |
|---|---|
| | proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 1.33 million. |
| *Type of Action* | Coordination and Support Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [74]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved protection of minors, including by more reliable age assessments and by minimising the use of intrusive age assessment methods;
- Improved adaptation, preparedness and cooperation of authorities in the fight against human trafficking;
- Expanded European-based knowledge on reliability, accuracy and effectiveness of age assessment methods.

[74] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Scope: Many unaccompanied children and young persons arriving at the external EU borders and seeking asylum, lack official documents showing their identity and age. Age assessment methods are important as they contribute to the determination of, for example, where an individual will be initially housed and what services, supports, and legal processes they will receive to ensure protection and, if applicable, child protection.

In other cases, minors are victim of trafficking of human beings (THB) criminal activities, either across the EU external borders, or within the EU borders. In other cases again, age assessment methods are necessary for law enforcement investigations on protecting children, forensic investigation, and/or the identification of victims.

No age assessment method can offer a 100% reliability. Different approaches have different sensitivity and specificity, and different sample sizes and representativeness, and some approaches are based on a non-European knowledge base. Furthermore, there is considerable variation in methods of age assessment. Methods may use approaches as diverse as interviews, psychological assessments and other holistic approaches; medical approaches such as X-rays, CT scans, DNA methylation, dental observation, or other analyses; other approaches such as image analysis; and they may use or not artificial intelligence (AI) for data analysis.

EU regulations, and guidelines by the European Union Asylum Agency (EUAA)[75], include safeguards and recommendations, such as that the least invasive methods should be used, and that medical methods should be used as a last resort. Further studies, reports or documents have also been elaborated by the European Migration Network[76], European networks of security practitioners for innovation, as well as at national level. The action funded by this topic should also consider these, as well as previous research, including but not limited to research by other relevant EU Framework Programmes projects.

This Coordination and Support Action should not develop methods or technologies of age assessment. Rather, it will analyse, including with practitioners, the current and potential methods for age assessment. It should assess and compare scientific reliability, sensitivity and specificity of different methods, as well as their potential risks for fundamental rights and how to minimize them.

While the research results would not imply any legislative or policy decision on age assessment methods, the research will develop evidence-based results on options for more (compared to the state-of-the-art) appropriate models of age assessment methods that protect fundamental rights, ensuring the use of an inclusive approach that addresses diverse needs. The results of research funded by this topic will contribute to capabilities for better identification of children and minors in the migratory, security, border management and other

[75] EASO Age assessment practices in EU+ countries: updated findings (europa.eu)https://euaa.europa.eu/sites/default/files/EASO_Age_assessment_practices_updated.pdf[

[76] https://ec.europa.eu/home-affairs/networks/european-migration-network-emn_en

contexts, following the principles of the EU Strategy on the rights of the child[77]. They will also contribute to the exchange of practices among European authorities.

Synergies with other Horizon Europe Cluster 3 Destinations, such as "Better protect the EU and its citizens against Crime and Terrorism" and "Disaster-Resilient Society for Europe", as well as with Destinations of Horizon Europe Cluster 2 "Inclusive Society".

**HORIZON-CL3-2027-01-BM-01: Open topic on research and innovation for effective management of EU external borders that promotes fundamental rights and EU values**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border, Coast Guard or Customs Authorities from at least 2 different EU Member States or Associated countries. For these participants, applicants must fill in the table "Eligibility information about practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of* | The rules are described in General Annex G. The following exceptions apply: |

[77] COM(2021) 142 final.

| | |
|---|---|
| *the Grant Agreements* | The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [78]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to the following expected outcome:

- Improved border management solutions that protect and promote fundamental rights of both EU citizens and Third Country Nationals.

Scope: Under this Open topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions that are not covered by the other topics of this Destination in 2026 and 2027.

In particular, this topic will fund research projects that explore, develop and test knowledge and technology solutions in the areas of border surveillance, border checks, customs and supply chain security, and civilian maritime and aviation security border management that protect and promote fundamental rights of both EU citizens and Third Country Nationals, and EU values.

Adapted to the nature, scope, type and target TRL of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing and validation of developed tools and solutions. Proposals should be convincing in explaining the methods they intend to use for demonstrating, testing and validating the proposed tools and solutions ensuring that the intersectional perspectives of diverse groups, including gender, sex, age, disabilities, race or ethnicity, sexual orientation and migrant status are integrated and considered. Proposals should also delineate the plans to develop possible future follow-up research and development and/or uptake, upscaling and/or application and use at national and EU level as possible next steps after the research project.

[78] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Research proposals should consider, build on if appropriate and not duplicate previous research, including but is not limited to research by other Framework Programmes' projects.

**HORIZON-CL3-2027-01-BM-02: Trusted, secure, quality future digital travel credentials**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions |

| | |
|---|---|
| | under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [79]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development, testing and integration of issuance, validation and sharing capabilities for possible future types (beyond Type 1) of Digital Travel Credentials (DTC);
- Integration of innovative, on-the-move, biometrics and remote biometric acquisition modalities to support the use of DTCs;
- Improved secure connectivity and interoperability for future DTCs;
- Improved capability of issuance of emergency travel documents and/or emergency DTCs.

Scope: Issuance, verification and management of digital travel credentials (DTCs) is relevant for border management, immigration and visa management. Furthermore, it could also be relevant to combat illicit activities such as terrorism, crime or frauds. This topic aims at supporting research and innovation that explore, develop and test enhanced capabilities for securely issuing, verify and manage (including sharing) possible future types of digital travel credentials (DTCs) for travel across the external borders of the EU.

The proposed solutions must be compatible with current, planned or foreseeable EU DTCs formats, and with applicable International Civil Aviation Organisation (ICAO) schemes, but they should also push forward to possible further types of DTCs (“Type 2” and “Type 3”).

Additionally, the funded actions should also work on the integration of current and new biometrics, and/or new biometric acquisition modality, in support of DTCs. This includes but does not limit to biometrics such as fingermark, palmprint, palmmark, rolled fingerprint, contactless fingerphotos, and biometric acquisition modalities such as remote and on-the-move, including those modalities developed by previous projects funded by this Destination of Horizon Europe Cluster 3. The project should develop and/or contribute to reference biometric sample quality assessments standards for these biometric modalities included in the DTCs, compatibly with existing relevant tools such as the Open Source Face Image Quality

[79] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under ‘Simplified costs decisions’ or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

(OFIQ), or improving forward-looking interoperability, for example between contact and contactless fingerprint data.

The funded research project(s) can also address the use case of verification, issuance or re-issuance of (emergency) DTCs in cases of emergencies (including evacuations of EU citizens).

Funded research can additionally address the security of breeder documents, which risk to be "weak links" when they are used to obtain genuine, secure travel credentials.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap; and on the engagement with the Agencies during the implementation of the project. At the stage of proposal preparation, Frontex and eu-LISA will not provide any guidance on, or otherwise be involved in the preparation of, project proposals. Proposals should consider and foresee that Frontex and eu-LISA may observe pilots and demonstrations when the project will be implemented, with the aim of facilitating future uptake of innovations for the border and coast guard community.

To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

**HORIZON-CL3-2027-01-BM-03: Detection and characterisation of threats or illegal/ smuggled goods in cargo**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 14.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks. |

| | |
|---|---|
| | The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Customs Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B. |
| *Procedure* | The procedure is described in General Annex F. The following exceptions apply:<br>To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one proposal that is the highest ranked within each of the two options: Option a, and Option b; provided that the applications attain all thresholds |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [80].<br>Beneficiaries must provide financial support to third parties. The support to third parties can only be provided in the form of grants. The maximum amount to be granted to each third party is EUR 100 000 to support the expected outcomes of the topic and effective collaboration and/or coordination with additional relevant national Customs Authorities, including testing and validation activities within the |

[80] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| | projects; the organisation of testing and validation activities also justifies the maximum amount to be granted to each third party indicated above. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Increased security of air, maritime, land, or postal transport, cargo and supply chain;
- Address accidental or intentional explosions, fires, noxious chemicals, material degradation, or autonomous threats in cargo;
- Enhanced capabilities to detect, characterise, track and trace, and seize dangerous, regulated, illicit devices, goods, or material;
- Increased mobility of the customs authorities' resources and equipment and improved agility for a faster and more coordinated response;
- Interoperability of customs control equipment and interconnectivity with other systems, including integration of logistical operations, and/or increased inter-agency and cross border collaboration.

Scope: Today's global economy and high-volume trade flows require much and fast transport to deliver products worldwide. Traders and consumers expect quick and easy transactions, while customs administrations face the challenge of controlling the goods without disrupting their flow. This is exploited by organised crime and terrorist organisations, which take advantage of the large amount of goods to conceal threats or illegal and/or dangerous materials in legal commercial cargo, with the aim of causing damage, disruption, or of it illegally crossing borders unnoticed.

Customs authorities must ensure a high level of compliance with both security and revenue objectives: trafficked materials may represent a threat, and undetected smuggled licit materials entering the EU deprive the Member States of the revenue due if the material had been legally traded. In addition, illegal trafficking can have an impact in the environment (such as biodiversity loss or deforestation) or for the EU citizens' safety and health.

The air and maritime cargo contexts present security challenges as well as high potential consequences of threats, primarily but not limited to explosives and incendiary devices. Air cargo can represent continuity assurances to cope, at least in the short term and for critical lines, with supply chain and/or distribution crises; while maritime cargo remains the most common transport mode in global trade. The risk for well-concealed materials not being detected during screening, or the risk of concealment during the supply chain is pressing.

Logistical hubs also need to strengthen their capabilities to adapt to sudden changes, and customs authorities need to mobilise their available resources to ensure efficient and fast controls. The need for better mobility and improved agility for customs is accompanied by the need to deploy scalable solutions, that are interoperable with other systems to facilitate co-sharing of equipment between BCPs and between Member States.

Innovation actions funded under this topic should develop and test solutions for cargo security, relevant to one or more transport modes (maritime, air, postal, road, or rail); and usable at one (or more) crucial point(s) of the supply chain. Innovation can also develop enhanced capabilities for customs to detect illicit, regulated and / or dangerous goods and transactions, and to be able to effectively characterise them in a timely manner. Improved tracking and tracing capabilities will facilitate the seizing of the materials while contributing to collecting data and evidence to further support investigations and prosecutions.

Proposals are expected to address one of the following options that should be explicitly selected:

**Option a:** security of cargo

**Option b:** detection of smuggled and trafficked goods/materials in cargo

Detection capabilities should target one or more type(s) of dangerous, illicit and/or illegal goods or materials, including: explosive or incendiary devices; illicit drugs and their precursors; illegally traded species, including covered by the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) and considering the Regulation on Deforestation-free Products[81]; illegally traded cultural property; contraband; trafficked weapons; chemical, biological, radiological, nuclear and explosive (CBRN-E) material or precursors; F-gases; and/or various modi operandi related to cross-border trafficking, including involving cargo.

Where the identification of illegal goods cannot be achieved without opening containers (for example, in the case of species or their parts), and where imagery, chemical, or molecular tests are required, appropriate measures should be established to reduce the response time between sampling and expert assessment, thereby minimizing disruption to the flow of goods.

Examples of technologies and approaches that can be explored by the research actions include (non-prescriptive and non-exhaustive): smart active defuse systems, sensors, artificial intelligence, tracking and tracing systems, distributed ledger technologies, non-intrusive inspection, automated threat recognition systems, and screening and scanning systems.

Equipment and technologies enabling increased security of cargo should contribute to cost and energy efficiency, limit their environmental impact and being more sustainable when they will be taken up in the future. An increased security of air cargo, furthermore, should not be regarded as an incentive to use air transport when this has a higher environmental and emissions impact, but prioritised on critical supply lines and/or situations.

81 https://environment.ec.europa.eu/topics/forests/deforestation/regulation-deforestation-free-products_en

Proposals received under this topic should demonstrate how the project would integrate the perspective for the whole supply chain, from load to delivery. Proposed solutions should be interoperable with the different relevant equipment and systems deployed by the customs authorities. Proposals should demonstrate how their solutions would align with existing interoperability standards (if any), and consider issues of cybersecurity and EU technological sovereignty and strategic autonomy. Proposals submitted under this topic are expected to align with the customs reform (if adopted) and customs policy priorities, and the projects should, once started, align with the policy priorities of the proposed EU Customs Authority and its Data Hub (if established).

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other relevant EU Framework Programmes projects on security research.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals. The results of the research should be taken up by EU customs authorities with the support of the Customs Control Equipment Instrument (CCEI) and/or subsequent funding opportunities, or the proposed EU Customs Authority and its Data Hub (once established).

Synergies within civil security can be an asset, for example with Better protect the EU and its citizens against Crime and Terrorism and Resilient Infrastructure.

**Destination - Resilient Infrastructure**

Following the Commission political guidelines 2024-2029 this Destination will support the implementation of the directives on the Resilience of Critical Entities (CER)[82] and on Network and Information Security (NIS2)[83]. Actions will focus on upgrading physical and digital security and resilience of critical entities and their supply chains, including the European strategic autonomy aspect.

Research and innovation investments will continue addressing emerging and existing challenges for critical entities, including hybrid threats. Cross-destination and cross-cluster cooperation will be fostered to better understand the risks, including technological, organizational and underpinning societal issues, and to deliver innovative, scalable, interoperable, long-lasting and effective tools to anticipate, prevent, detect, monitor, manage and investigate them. These actions will contribute to realising the objectives of the ProtectEU – a European Internal Security Strategy[84], Counter-Terrorism Agenda[85] and the European Preparedness Union Strategy[86].

Furthermore, this Destination will continue to develop measures to improve the resilience, safety, and security of urban and peri-urban areas against deliberate or accidental human actions, preserving citizens' right to feel safe and have access to essential services, while meeting climate resilience objectives of the EU Adaptation Strategy[87].

Projects funded under this Destination will promote technological and social innovations enhancing the sovereignty, competitiveness and strategic autonomy of European critical entities, authorities and operators including their respective supply chains. Moreover, submitted proposals should consider current policy developments and meet expectations of the following EU legislation and policy documents, whichever would be relevant to the challenges addressed by the proposal:

- EU Cybersecurity Strategy[88];
- EU Maritime Security Strategy[89];
- EU Aviation Security Strategy[90];
- Europe-wide Climate Risk assessment (EUCRA) and Commission Communication on Managing Climate Risks;

82 Directive (EU) 2022/2557.
83 Directive (EU) 2022/2555.
84 COM/2025/148 final
85 COM (2020) 795 final.
86 JOIN(2025) 130 final
87 COM (2021) 82 final.
88 JOIN (2020) 18 final.
89 Council of the EU 11205/14 JOIN(2023) 8 final.
90 REGULATION (EC) No 300/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

- European Economic Security Strategy[91];
- Joint Framework on Countering Hybrid Threats[92] and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats[93];
- EU C-UAS Strategy[94];
- EU Space Strategy for Security and Defence[95];
- EU Disaster Resilience Goals[96];
- European Preparedness Union Strategy[97];
- EU Action Plan on Cable Security[98];
- European Water Resilience Strategy[99].

To this end, these proposals should contribute to the achievement of one or more of the following generic impacts:

- physical and/or digital aspects of critical entities safety and security are considerably improved, while dependencies on non-European technologies, services, and resources are significantly reduced;
- new and upgraded systems support the interoperability enabling rapid response and recovery from complex security incidents without significant human involvement, and situational awareness and information sharing functionalities are available, especially where emergency responders' intervention is required;
- security-by-design, preparedness-by-design and where relevant circularity-by-design are default features of both newly created and upgraded infrastructure;
- urban, peri urban areas are more resilient through technological, organisational, and social innovations, and deepened public involvement;
- European citizens awareness and reaction capabilities in case of critical infrastructure disruption is considerably raised.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects.

---

91 JOIN(2023) 20 final.
92 JOIN (2016) 18 final.
93 JOIN (2018) 16 final.
94 COM (2023) 659 final.
95 JOIN (2023) 9 final.
96 (2023/C 56/01); COM (2023) 61 final.
97 JOIN(2025), 130 final.
98 JOIN(2025) 9 final.
99 https://circabc.europa.eu/ui/group/1c566741-ee2f-41e7-a915-7bd88bae7c03/library/b560bc22-6a61-4b63-b62b-a7fe890ea177/details

It will be important also to take into account how research results can be advanced to deployable solutions after the projects lifetime, utilising validation and capacity-building programmes like the Internal Security Fund, Digital Europe Programme and other.

Where possible and meaningful, synergy-building and clustering initiatives with successful actions in the same, or other relevant areas. should be considered, including the organisation of international events in coordination with the Community for European Research and Innovation for Security (CERIS)[100].

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2026-01-INFRA-01: Tools and processes to support stress tests of critical infrastructure**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.835 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.67 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The Joint Research Centre (JRC) may participate as member of the consortium selected for funding as a beneficiary with zero funding, or as an associated partner. The JRC will not participate in the preparation |

[100] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

| | |
|---|---|
| | and submission of the proposal - see General Annex B.<br>The following additional eligibility conditions apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios:<br>• critical infrastructure operator,<br>• authority responsible for critical infrastructure resilience,<br>• civil protection authority,<br>• law enforcement or private companies providing security for critical infrastructure.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [101]. |
| *Security Sensitive* | Some activities resulting from this topic may involve using classified |

[101] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Topics* | background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

- Critical infrastructure operators and authorities have access to efficient, adaptable, resilient and reliable tools and processes enabling or improving virtual and physical stress tests of their respective assets/ and operations;
- Critical entities have broader and deeper understanding of their technical and operational vulnerabilities and adaptive capabilities, improving the scenario building and stress tests exercises;
- Systems allowing notification and collaboration under stress conditions are available for relevant stakeholders;
- Critical entities are better equipped for post-incident investigations, including data collection, analysis and improved learning, management and sharing in a secure manner;
- Improved operational procedures including incidents management and training curricula are developed.

Scope: The resilience of critical entities is of paramount importance as disruptions to these systems can have significant consequences for the whole economy, public health, security or safety. These systems, responsible for providing essential services for modern society, are increasingly complex and interconnected, making them vulnerable to a range of threats, including cyber-attacks, physical attacks, malfunctions, human-induced or natural disasters.

The objective of this topic is to facilitate the stress testing of critical infrastructure by providing specialized tools and methodologies and support validation. This will enable the identification and testing of technical and operational vulnerabilities, inform of effective solutions to mitigate these risks, and facilitate the collection and analysis of data to enhance resilience plans that shall be established by each critical entity. Building on the insights gained from previous exercises, the ultimate goal is to establish more robust and comprehensive stress testing protocols, thereby ensuring the reliability and integrity of critical infrastructure.

The proposed solutions may, among others, support simulation and modelling, multi-hazard and multi-threat scenario building, data analytics, including geospatial information, Digital Twins, assessment of risks and adaptive capabilities, as well as impact of human factors.

These solutions should be designed to be inclusive and accessible, considering the needs of diverse users and stakeholders. Solutions should allow flexible configuration taking into account the evolving nature of threats and hazards. If feasible they should also be adaptable to different sectors and should support stress testing under diverse environmental and

geographical conditions, including operation in harsh and remote environments. Moreover, they should comply with the relevant legislative frameworks and allow application of the developed tools under the current regime taking into account the sensitivity and confidentiality of the processed information.

Coordination among the successful proposals from this topic and projects funded under HORIZON-CL3-2025-01-INFRA-01: *Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures* and HORIZON-CL3-2025-01-INFRA-02: *Open topic for role of the human factor for resilience of European critical entities*, should be envisaged in order to avoid duplication, share resources and exploit complementarities and opportunities for increased impact.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Where relevant, funded projects are encouraged to liaise with the European Commission's Joint Research Centre, for complementary real-scale testing at the Reaction Wall and HopLab of the European Laboratory for Structural Assessment (ELSA).

**HORIZON-CL3-2026-01-INFRA-02: Security challenges of the green transition in urban und peri urban areas**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 4.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific focus of the proposal submitted, these practitioners should represent one or several of the following portfolios:<br>• critical infrastructure operator,<br>• authority responsible for critical infrastructure resilience, |

| | |
|---|---|
| | • civil protection authority,<br>• safety or security first responders,<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [102]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

- Identification and analysis of potential new security risks related to innovative technologies being deployed in the urban and peri-urban environments;

[102] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Innovative and modern tools to identify and measure changes in urban and peri-urban areas caused by the green transition, insofar as they concern security and possible resilience approaches;
- Verification of measures countering potential safety and security risks, hazards and challenges arising in areas hosting green technologies;
- Contribution to building awareness and societal acceptance for the safety and security aspects of the green transition;
- Impacts of incidents involving new and emerging technologies are examined, including environmental and climate risks;
- Security, safety and resilience aspects of the supply chains of green technologies are analysed, including the technological and resource dependencies, and their aligning with the European strategic autonomy principle;
- Authorities and critical infrastructure operators are equipped with efficient evaluation methodologies for safe and secure deployment and integration of new and emerging technologies into urban and peri-urban areas.

Scope: Climate change and environmental degradation are an existential threat to the world, and the green transition is a critical component of the EU's strategy to reduce and mitigate their impacts, as well as to contribute to the European competitiveness. This approach is also part of the effort to transform Europe into a modern, resource-efficient, resilient and competitive economy. However, rapid deployment of new and emerging technologies, such as, but not limited to: green and grid-interactive roofs and walls, solar power installations, electric vehicle charging stations, energy storages, smart sensors and surveillance systems, green transportation systems, nature-based or other sustainable or reused construction materials, or specific infrastructure solutions may create security risks through new interdependencies including legacy infrastructure, the accumulation of deployed solutions, or otherwise create new potential risks and hazards of unknown scale and origin are an existential threat to the world, and the green transition is a critical component of the EU's strategy to reduce and mitigate their impacts, as well as to contribute to the European competitiveness. This approach is also part of the effort to transform Europe into a modern, resource-efficient, resilient and competitive economy. However, rapid deployment of new and emerging technologies, such as, but not limited to: green and grid-interactive roofs and walls, solar power installations, electric vehicle charging stations, energy storages, smart sensors and surveillance systems, green transportation systems, nature-based or other sustainable or reused construction materials, or specific infrastructure solutions may create security risks through new interdependencies including legacy infrastructure, the accumulation of deployed solutions, or otherwise create new potential risks and hazards of unknown scale and origin.

Proposals submitted under this topic should investigate the integration of *sustainable & environmentally friendly technologies* into urban and peri-urban areas to identify and explore physical and cyber risks and vulnerabilities resulting from this phenomenon, including, but

not limited to: battery fires, toxic leaks, electric shocks, structural integrity, toxic waste, data privacy, land management disruptions, including potential negative impacts on the natural environment, or social and community tensions. The proposals should also consider the threat of malicious access, software and data manipulation and misuse of managing systems potentially leading to harm to health, loss of life, environmental damage or economic damage, regardless of whether the intention is criminal, vandalism, hybrid attack or other.

The ultimate goal of this research is to inform operators, first responders and authorities on how to mitigate risks, enhance their preparedness and improve their response to potential incidents. By recognizing emerging threats, it should be possible to prevent major incidents from occurring, and in the event of an accident, provide effective strategies, managerial advice, processes and methodologies to respond and recover. The research should provide recommendations that are tailored to diverse communities and context needs such as those with different socio-economic profiles, adapted to people of different ages and genders to identify and mitigate physical and cyber risks and vulnerabilities. Proactively addressing major safety and security risks associated with the green transition will help to future-proof these technologies, build public trust, and promote their widespread acceptance, backed by evidence-based safety and security policies.

The proposed research should provide a comprehensive understanding of adaptive capabilities, the risks and vulnerabilities associated with *green technologies*, as well as practical recommendations for mitigating these risks and ensuring their safe, resilient and secure deployment while utilising the nature-based solutions and respecting principles of biodiversity. By doing so, it will contribute to the development of a resilient and sustainable urban environment, where the benefits of green technologies can be fully realized while minimizing their potential risks and negative impacts.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

**HORIZON-CL3-2026-01-INFRA-03: Targeted innovative capabilities for the resilience of critical entities to natural and human-induced disasters, including hybrid scenarios**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Innovation Actions |

| | |
|---|---|
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios:<br>• critical infrastructure operator,<br>• authority responsible for critical infrastructure resilience,<br>• civil protection authority,<br>• first responders' organisations or agencies,<br>• authority in charge of managing NaTech (Natural Hazard Triggered Technological) events,<br>• law enforcement or private companies providing security for critical infrastructure.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for |

| | |
|---|---|
| | Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [103]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

- Improved understanding of systemic vulnerabilities of critical entities including physical, digital, operational, and cross-sectoral dimensions, in the face of compound natural and human-made disaster risks;
- Verification of existing measures countering potential NaTech risks;
- Demonstration of advanced technological solutions that enhance the ability of public and private providers of critical services to prepare for, respond to, and recover from complex, multi-hazard scenarios, including cascading or hybrid NaTech events;
- Deployment of common platforms and operational tools for dynamic risk assessment, decision support, between public authorities, first responders, and critical infrastructure operators during disruptive events;
- Strengthened multi-level and cross-border cooperation frameworks for integrated emergency and continuity management, ensuring seamless coordination across sectors, governance levels, and jurisdictions.

Scope: Recent compound and cascading disasters have demonstrated the urgent need to reinforce the resilience of critical entities against a wide spectrum of hazards, including both human-induced incidents, natural events such as floods, wildfires, earthquakes, and storms, and natural hazard triggered technological (NaTech) accidents, including hybrid scenarios. The vulnerability of key infrastructures is exacerbated by their growing interdependencies and the systemic propagation of risks across sectors and borders. In this context, ensuring the monitoring, protection and continuity of essential services has become fundamental to preserving and enhancing societal resilience.

This topic aims to support the development and demonstration of targeted high-tech capabilities that address specific preparedness, operational, and recovery gaps in the resilience

[103] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

of critical entities[104] under multi-hazard and NaTech conditions. It calls for moving beyond generic resilience frameworks toward sector-specific, interoperable, and modular technological and governance solutions that can be deployed and tested in realistic operational settings.

Proposals should be grounded in existing risk assessments and draw on lessons learned from recent disruptive events. They are expected to deliver measurable improvements in both technological and organisational resilience through the identification and prioritisation of critical capability gaps, especially where cascading and cross-sectoral risks are likely to arise. In parallel, adaptive continuity planning and decision-making tools should be designed to enhance situational awareness, support dynamic response coordination, and maintain service continuity in fast-evolving crisis scenarios.

Proposals should also demonstrate cross-border, multi-actor coordination mechanisms through simulations or testing in real operational environments, involving public authorities, emergency responders, and critical service operators or representative environments where critical infrastructure is particularly exposed to multi-hazard risks.

International cooperation is encouraged, particularly in regions with cross-border infrastructure or shared vulnerabilities. Actions should take due account of the relevant EU legal and policy frameworks and are expected to address all applicable considerations expressed in the Introductions of the Resilient Infrastructure and Disaster-Resilient Society for Europe Destinations.

Coordination among the successful proposals from this topic and projects funded under HORIZON-CL3-2025-01-INFRA-01: *Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures* and HORIZON-CL3-2025-01-INFRA-02: *Open topic for role of the human factor for resilience of European critical entities*, and HORIZON-CL3-2024-DRS-01-04: *Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster* should be envisaged in order to avoid duplication, share resources and exploit complementarities and opportunities for increased impact.

**HORIZON-CL3-2027-01-INFRA-01: Enhancing physical protection of critical infrastructures**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a |

[104] Including, but not limited to, infrastructures addressed by the revised EU Maritime Security Strategy (JOIN/2023/8) and the European Port Strategy.

| | |
|---|---|
| | proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 12.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility conditions apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios:<br>• critical infrastructure operator,<br>• authority responsible for critical infrastructure resilience,<br>• civil protection authority,<br>• law enforcement or private companies providing security for critical infrastructure.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, |

| | |
|---|---|
| | as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [105]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

- Critical infrastructure operators and authorities have improved physical risks and hazards assessment capabilities;
- Perimeter security, access control, surveillance systems, remote sensors and other systems used by or relevant to critical infrastructure operators are capable of coping with threats from misuse of new and emerging technologies;
- Improved operational procedures, including incidents management and training curricula, are developed;
- Innovative solutions for critical infrastructure resilience are being developed, utilising recent advancements in spatial planning, security-by-design, preparedness-by-design and nature-based solutions using an inclusive approach that address diverse needs.

Scope: Physical protection of critical infrastructure should keep up its advancement to match risks and hazards stemming from malicious use of new and emerging technologies, and evolving operational environment, as well as improve its safety and security measures against knowns and emerging threats. Following this approach entities providing essential services should reduce their vulnerability, among others, to threats from improvised explosive devices, ramming attacks, sabotage, uncooperative and hostile unmanned platforms including swarm robotics, penetration of access points by unauthorised individuals and vehicles, unauthorised access to hazardous material storage, removal of critical components, or deterioration of critical infrastructure due to age, inadequate design or changed operational conditions, including climate.

[105] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Proposals submitted under this topic should identify and analyse possible new challenges for the physical security of the critical entities and develop adequate tools, recommendations, manuals and training programmes for relevant operators and authorities. Where relevant for their scope proposals should utilise the nature-based solutions and respect principles of biodiversity. Furthermore, solutions should take into account interdependencies in the context of supply chains and their impact on physical protection.

Coordination among the successful proposals from this topic and projects funded under HORIZON-CL3-2025-01-INFRA-01: *Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures* and HORIZON-CL3-2025-01-INFRA-02: *Open topic for role of the human factor for resilience of European critical entities*, should be envisaged in order to avoid duplication, share resources and exploit complementarities and opportunities for increased impact.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

**HORIZON-CL3-2027-01-INFRA-02: Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.835 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 7.67 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility conditions apply:<br>This topic requires involvement as beneficiaries of at least 3 relevant |

| | |
|---|---|
| | practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios:<br>• critical infrastructure operator,<br>• authority responsible for critical infrastructure resilience,<br>• law enforcement or private companies providing security for critical infrastructure.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [106]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to some or all of the following outcomes:

[106] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Critical infrastructure operators and authorities have improved awareness of Open-Source Intelligence (OSINT) and their potential impact on security of their operations;
- Toolbox for OSINT mapping, including enhanced analysis and risk flagging is developed and available to relevant stakeholders;
- Critical infrastructure operators and authorities have improved incident response, emergency plans and business continuity models;
- Removal of potentially harmful OSINT from the public domain in order to counter/prevent preparations and attempted attacks against critical entities, including the lone wolf and hybrid scenarios;
- Awareness campaigns and training curricula for critical entities' employees are developed.

Scope: The malicious use of Open-Source Intelligence (OSINT) is a known concern and technique used by offenders to retrieve personal, professional, and official or technical information about entities and their employees either to immediately plot illegal actions or use it to access more sensitive data with social engineering techniques like tailored data phishing. Although singular information may seem harmless, their critical mass coupled with reasoning and automated processing of large data blocks, could reveal critical vulnerabilities and possible attack vectors. This modus operandi is of special concern for critical infrastructure operators and authorities, as it can be used to aggregate sensitive information, identify potential protection gaps, discover the security measures, such as camera and sensor locations or target individuals with special access privileges in order to orchestrate more sophisticated and harmful attacks. OSINT can also be used to impede critical infrastructure operations indirectly, gathering information and affecting their supply chains.

Proposals submitted under this topic should analyse the type, amount and accessibility of publicly available information and their usefulness in planning hostile operations against critical entities and their services. They should also parse the role of OSINT for identification and recruitment of insiders, identity theft, impersonation, or launching psychological operations such as foreign information manipulation and interference or disinformation. Moreover, the implications of AI data processing to misuse OSINT potential should be addressed. Any potential OSINT sources should be covered including, but not limited to social media, online fora, cloud resources, public records and databases, lawfully accessible deep web and dark web data, geospatial information, as well as paper archives in the public domain with blueprints, emergency response plans or similar. Proposals should especially consider scenarios including hybrid threats and lone wolves and develop tools and awareness campaigns to mitigate such threats.

Proposals should build upon outcomes and tools of other relevant projects, adapting, optimising and integrating them when necessary to achieve the highest possible technology readiness level of the project results. The proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including

validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

## Destination - Cybersecurity

Cybersecurity is essential for safeguarding Europe's digital sovereignty, resilience, and technological leadership. The Horizon Europe Work Programme for Cybersecurity 2026-2027 builds on the broader EU strategic vision for cybersecurity as articulated in the EU Cybersecurity Strategy for the Digital Decade and contributes directly to the implementation of major initiatives including the Cyber Resilience Act, NIS2 Directive, Cyber Solidarity Act, AI Act, and the EU Quantum Strategy. It complements the deployment-focused Digital Europe Cybersecurity Programme, ensuring continuity from research and innovation to operational capability across the cybersecurity ecosystem.

The Cybersecurity actions proposed under this destination as described in the Annexes, are designed to reinforce the EU's ability to detect, prevent, and respond to cyber threats, including those targeting critical infrastructure. Furthermore, they contribute to Europe's open strategic autonomy by supporting the development of trustworthy digital infrastructures, emerging technologies, cybersecurity capabilities, and secure supply chains.

The strategic plan 2025-2027 identifies the following impact: "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".

Under this Work Programme, the Commission intends to conclude a contribution agreement entrusting the European Cybersecurity Competence Centre (ECCC) with the implementation of call topics related to Increased Cybersecurity. Please refer to "Indirectly managed action by the ECCC" in the section "Other Actions" of this Work Programme part – including the Appendix providing the call specifications for information purposes. Those specifications incorporate 'expected outcomes' set out below.

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

## Destination - Disaster-Resilient Society for Europe

Given the increasing frequency and ever greater impacts of disasters resulting from climate extremes, natural, geohazards and human-made hazards, the EU needs to invest more in improving disaster risk management, tools for disaster management[107] and societal resilience to avoid creating new exposure; reduce existing risk by building up resilience, prevention and preparedness; manage residual risk. In this respect, along the orientations given in the Horizon Europe strategic plan 2025-2027, the main objectives of this destination supporting the reduction of losses from natural, accidental and human-made disasters will be pursued in continuity with the strategic plan 2021-2024.

This destination will support the implementation of the European Commission political guidelines 2024-2029 for a 'Safer and more secure Europe', a 'Preparedness Union', with 'Stronger Common Borders', protecting democracy and putting research and innovation at the heart of a resilient economy. The European Preparedness Union Strategy[108] is a key document in its implementation. Overall, research under this Cluster should continue to focus on preserving and securing citizens' basic right to feel safe. This destination will support the European Commission efforts towards:

- enhancing efforts to prevent and prepare for new threats, especially those linked to chemical, biological, radiological and nuclear (CBRN) security.
- continuing to address risks to security from climate change impact / step up work on climate resilience and preparedness.
- supporting medical countermeasures against public health threats.

Moreover, this destination will support the implementation of UN Disaster Risk Reduction policies, the EU Disaster Resilience Goals[109] involving closer coordination with the Union Civil Protection Knowledge Network, the rescEU initiative and Member States' civil protection authorities, as well as an enhanced dialogue at international level with the United Nations Office for Disaster Risk Reduction (UNDRR) on recommendations for the Sendai Framework[110] and United Nations Sustainable Development Goals (SDGs). Such closer coordination with other programmes will make it possible to further streamline future research programming. For example, Cluster 3 should focus on its core added value, which is a strong operational character for preparedness, crisis management, response and learning, while maintaining complementarities with broader prevention issues such as climate-related risks, covered by Cluster 5, and the Mission on Climate Change Adaptation. There are similar

---

107 Disaster management refers here to systems for preventing, preparing for and responding to natural and man-made disasters in the spirit of Decision No 1313/2013/EU. The protection they provide shall cover primarily people, but also the environment and property, including cultural heritage, against all kinds of natural and man-made disasters, including the consequences of acts of terrorism, technological, radiological or environmental disasters, marine pollution, hydrogeological instability and acute health emergencies, occurring inside or outside the Union. In the case of the consequences of acts of terrorism or radiological disasters, it should cover only preparedness and response actions.

108 JOIN(2025) 130 final.

109 COM/2023/61 final.

110 UNDRR, Sendai Framework for Disaster Risk Reduction 2015-2030.

examples in closer coordination with Cluster 6 and the One Health approach, regarding, for instance, water and food security threats (as a result of intentional degradation or terrorist acts).

From a technological perspective, the Destination will ensure greater involvement of practitioners in close cooperation with the Member States and EU agencies, not only in research development and implementation, but also the identification of gaps and needs and future research topics. Actions to develop tools and technologies to meet operational capability needs should be aimed at higher technological readiness levels (TRLs). Finally, it will be important to take into account how research results, both those still to come and those already developed in past projects under the DRS destination, can be turned into deployable solutions by being combined with capacity-building programmes (in particular the Internal Security Fund, funding under the Union Civil Protection Mechanism [111], the European Regional Development Fund, and the Cohesion Fund), and social innovation to support the entry into the market of developed technologies. Actions will also aim to ensure that there is a link between R&I and possible procurement (e.g., in the area of medical countermeasures).

Proposals for topics under this Destination should have the overarching objective of improving resilience. Actions will continue to explore initiatives and experiments involving the development of technological or methodological solutions for crisis management and support for emergency responders, getting the general public more involved in this area and improving interactions between regional and/or local authorities, public practitioners, private operators and civil society. Actions could also take into consideration human induced environmental disasters and regions vulnerable to extreme weather events in coastal areas, sea level rise and other climate change impacts, which may prone to disaster risks (e.g. the Arctic). New tools or solutions should build on what has been developed in past projects and be capable of being integrated into existing (legacy) systems. Actions will also focus on multi-service capability developments, in particular tools and technologies to support direct operational needs in case of a disaster. This will be done in a scalable way, covering areas from small rural towns to economically developed ones with a high population density, and opening research initiatives to international cooperation. Capabilities need to be upgraded to match the new resilience stakes and expectations of practitioners and of society as a whole. We should learn from past disaster events by identifying gaps in capabilities that the response to such events showed were lacking. For example, one of such gaps are the availability and distribution of medical countermeasures used to effectively respond to deliberate or accidental releases of CBRN-E substances.

The destination will continue to follow a multi-hazard approach, addressing disasters and threats of all kinds, including their cascading issues, climate-related or natural or human-made and geological hazards, industrial accidents, pandemics, intentional hostile acts including terrorism and armed conflict. Particular attention will be paid to floods and wildfires, as well as to chemical, biological, radiological, nuclear and explosive (CBRN-E) threats. To this end, proposals should contribute to the achievement of one or more of the following impacts:

[111] See the UCPM scientific needs assessment on disaster risk management: https://civil-protection-knowledge-network.europa.eu/media/outcome-report-scientific-research-needs-exercise

- Enhanced citizen and regional and/or local authorities' involvement in research actions, and in operational measures that may result from research, with focus on risk awareness and enhanced disaster prevention and preparedness, adapted to all types of disability (sensorial, physical, intellectual), including youth awareness raising and education;

- Improved disaster risk governance (from prevention, preparedness to mitigation, response, deployment of countermeasures and recovery, using updated risk assessment methods and decision criteria, and including knowledge transfer and awareness of innovative solutions) from international to regional and/or local levels;

- Strengthened capacities of disaster management systems for preventing, preparing for and responding to natural and human-made disasters in the spirit of Decision No 1313/2013/EU [112] including development of new prevention or preparedness technologies, infrastructures or assets as well as in support of field operations with validation of tools and technologies used in disaster responses including emergencies, and demonstration of their interoperability.

More precisely, in the context of exacerbated impacts of various disaster threats on vulnerable societies, research and innovation actions are highly needed to face the many challenges faced by European Society. Some of them are:

- Challenges related to inclusion of the general public, regional and/or local communities and voluntary organisations as active partners in order to:

    - Empower citizens to act and help them to improve their disaster risk awareness and own resilience to crises, including accountability for regional and/or local administrative decisions on residual risks, youth awareness raising and education;

    - Provide all actors involved in the management of natural disasters, human-made emergency situations, and humanitarian crises with timely and accurate geo-spatial information derived from satellite remote sensing and completed by available in situ or open data sources in all phases of the emergency management cycle: preparedness, prevention, disaster risk reduction, emergency response and recovery, as well for early warning and in emergency situations;

    - Provide means for regional and/or local decision-makers and operational responders, i.e., first and second responders. A “second responder” is a worker who supports "first responders" such as police, fire, and emergency medical personnel. They are involved in preparing, managing, returning services, and cleaning up sites during and after an event requiring first responders, including crime scenes and areas damaged by fire, storm, wind, floods, earthquakes, or other natural hazards.

[112] Under the Decision, the protection they provide shall cover primarily people, but also the environment and property, including cultural heritage, against all kinds of natural and human-made disasters, including the consequences of acts of terrorism, technological, radiological or environmental disasters, marine pollution, hydrogeological instability and acute health emergencies, occurring inside or outside the Union. In the case of the consequences of acts of terrorism or radiological disasters, it should cover only preparedness and response actions.

These types of services may include utility services (shutdown or reinstatement of electrical, gas, sewage, and/or water services), wireless or wireline communication services, specialty construction (i.e. shelter construction), hazardous waste clean-up, road clearing, crowd control, emergency services (i.e. Red Cross[113], first aid, food services, security services, social services (i.e., trauma counsellors), and sanitation, infrastructure owners, regional and/or local authorities (including public services, transport and utilities) to coordinate prevention and preparedness actions, bearing in mind the socio-economic and cultural context, and for operational responders to influence regional and/or local planning decisions that affect exposures and vulnerability to risks in short and long term;

- Address citizens' perception of, and involvement in, civil defence in the event of very large-scale disasters including armed conflict.

- Challenges regarding the reinforcement of disaster risk governance and the consideration of knowledge and innovative solutions in order to:
  - Improve operational management of crises at different levels (prevention, preparedness, response, recovery) and scales (international to regional and/or local),
  - Reinforce the uptake and transfer of knowledge to risk managers, first and second responders and decision-makers;
  - Strengthen resilience and enhancing protection strategies for emergency services and healthcare workers in case of disasters;
  - Reinforce civil defence capability, looking at all facets of crisis and disaster management, alongside community resilience building;
  - Enhance preparedness for optimised detection, prevention, response and control measures in case of bioterrorism or emerging diseases.
- Challenges related to wildlife- and domestic animals protection against disasters.
- Challenges related to the validation and usability of tools and technologies, including the demonstration of their interoperability, in the context of strengthened cross-sectorial disaster management capacities as to:
  - Enhance risk awareness, preparedness and communication about foreseeable impacts of disasters;
  - Deploy innovative solutions in emergency situations including trusted communication channels (considering the upcoming proposal for a European Critical Communication System), emergency medical response, including triage of

[113] https://redcross.eu

victims, pre-hospital and clinical services, medical countermeasures, support equipment (e.g. detectors), as well as protection of first responders;

- Coordinate and further develop awareness and early systems for floods, wildfires, droughts, etc., considering Earth observation and modelling (Including the Copernicus Emergency Management Service), space communication (IRIS$^2$), space navigation (Galileo and the Galileo EWSS Early Warning Satellite System), while ensuring alignment with the technical and scientific requirements to guarantee interoperability;

- Enhance validation of tools, technologies and processes for cross-border prevention, decision-support and responses to climate-related and geological disasters and emergency crises by different practitioner sectors (firefighters, medical emergency services, civil protection, police, NGOs);

- Enhance interoperability of tools and technologies used in international emergency (real-case) situations related to natural hazards, CBRN-E threats and hybrid threats via inputs such as standard operating procedures for foresight, risk analysis or guidance with the aim to improve market uptake.

This Destination will also support, whenever appropriate and applicable, the proposals with some or all of the following goals:

- a clear strategy from international to regional and/or local on how the overall society will adapt to the evolving disaster risks based on the subsidiarity principle (from the citizen level to international decision-making);

- the involvement of different disaster risk management stakeholders and regional and/or local authorities in research, development and validation of methods and tools;

- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);

- the active involvement of Small and Medium Enterprises (SMEs);

- a robust plan on how they will build on the relevant predecessor projects, and clustering with existing research (EU and national) actions to maximise complementarities and synergies and avoid duplication of efforts;

- education and training aspects for first and second responders for different types of threats (climate-related, geohazards, accidental, intentional), and adapted to all types of disability (sensorial, physical, intellectual, as well as information sharing and awareness raising of the citizens;

- a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders, taking into consideration the final users and the usability of the outcomes after the end of the project;

- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS)[114] activities and/or other international events.

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2026-01-DRS-01: Designing new ways of risk awareness and enhanced disaster preparedness**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>Due to the scope of this topic, relevant international organisations with headquarters in a Member State or Horizon Europe Associated Country are exceptionally eligible for funding.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 organisations from at least 3 different EU Member States or Associated |

[114] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

| | |
|---|---|
| | Countries as follows: (i) at least one civil society organisation (CSO); (ii) at least one authority in charge of disaster risk[115] (iii) at least one organisation representing local or regional authorities. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [116]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of innovative tools and methodologies to monitor and improve risk awareness across society, integrating diverse community perspectives and leveraging advanced technologies;

115 Authorities in charge of disaster risk entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement national disaster risk prevention, preparedness or response measures.

116 This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Development and uptake solutions and tools for the successful increase of safety culture and societal resilience of communities with concrete material, while considering also the inclusion and protection of marginalized populations in disaster scenarios;

- Creation of comprehensive, inclusive preparedness plans that involve all societal sectors and governance levels, ensuring coordinated and effective responses to disasters (such as from early warning to early action), including scarcity of resources;

- Establishment of a resilient, adaptive response framework that enhances collaboration between public authorities, communities, and private sectors, improving overall disaster resilience.

Scope: Building on the whole-of-society and whole-of-government approach, this topic should contribute to enhancing risk awareness and disaster preparedness through the development of innovative tools, methodologies, and frameworks. A key focus should be on integrating diverse societal and resilience perspectives considering people in a vulnerable situation, ensuring inclusive participation in risk communication strategies, and leveraging accessible advanced technologies and processes to improve public understanding of hazards and vulnerabilities (such as gender, disabilities and others social factors. and capabilities. Efforts should aim at designing and validating novel approaches to risk perception, communication, including digital platforms, immersive technologies, and participatory tools that foster citizen engagement and behavioural change, as well as wildlife protection. Behavioural insights should inform the projects on effective methods in population's preparedness including the risk communication. Special attention should be given to marginalized or vulnerable groups in a vulnerable situation ensure equitable access to risk information and preparedness resources.

To strengthen disaster preparedness and response capabilities across Europe, there is a clear need for an innovative, interoperable solution that enables the development of new strategies for risk awareness and disaster management. Such a solution should facilitate seamless collaboration between public authorities, civil society, local communities, and the private sector. It must support the co-creation of comprehensive preparedness plans that ensure a coordinated, robust, resilient, and effective response to a wide range of disaster scenarios. Central to this approach should be the integration of a command-and-control system that allows for centralized information management, efficient coordination among all stakeholders, and rapid, data-driven decision-making in emergency situations. For example, efforts to guarantee early action from early warning should be taken into account.

Furthermore, proposals should work towards the creation of comprehensive, multi-stakeholder preparedness plans that involve all levels of governance, civil society, the private sector, and local communities. These plans should establish mechanisms for cross-sectoral coordination, efficient resource allocation, and effective decision-making in crisis situations and the development of solutions and tools to ensure a greater culture of safety and societal resilience in the communities. Research should also explore innovative governance models that enhance interoperability and cooperation between different entities. To strengthen

disaster resilience, proposals should develop and test adaptive response frameworks that enhance collaboration between public authorities, civil society, communities, and businesses. These frameworks should incorporate near real-time risk assessment tools, digital simulations, and scenario-based exercises to improve the capacity to anticipate, respond to, and recover from disasters. The integration of AI-driven decision-support systems, taking into account existing biases, digital twin technologies (including Destination Earth), and predictive analytics could further contribute to a more effective, evidence-based crisis response.

Projects are expected to contribute to the overall enhancement of societal resilience by fostering a culture of preparedness, strengthening community-driven disaster risk reduction initiatives, proactive engagement in prevention- and mitigation of disaster's effects, and ensuring that all actors within society have the necessary tools and knowledge to respond effectively to future crises.

Where relevant, projects may take into account the assets, but also particular challenges faced by the European outermost regions and may include entities from these regions in the consortium's composition.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities.

International cooperation in this topic is strongly recommended. Proposals should also take into account lessons learned from past disasters and align with existing EU policies, frameworks, and international commitments in the field of disaster risk reduction and crisis management. Especially the population preparedness chapter of the Preparedness Union Strategy, such as the preparEU initiative, should be considered. Finding synergies with projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[117], is recommended.

**HORIZON-CL3-2026-01-DRS-02: Multi-hazard approach and cumulative / cascading impacts**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |

[117] Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

| | |
|---|---|
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>Due to the scope of this topic, relevant international organisations with headquarters in a Member State or Horizon Europe Associated Country are exceptionally eligible for funding.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 authorities in charge of disaster risk or crisis communication[118] and 2 representatives of local or regional authorities in charge of disaster response from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the |

[118] Authorities in charge of disaster risk or crisis communication entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement national disaster risk prevention, preparedness, response, or crisis communication measures.

| | |
|---|---|
| | Research and Training Programme of the European Atomic Energy Community (2021-2025) [119]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Integrated single-hazard systems into multi-hazard next generation predictive models to assess cascading effects (e.g., heatwave, floods, droughts, landslides, heavy rain) and interactions across meteorological, geophysical, and technological hazards;
- Enhanced hazard forecasting and response through research on model integration and platform interoperability;
- Development of holistic risk and resilience metrics to support multi-hazard prevention strategies, encompassing main physical, economic and social effects;
- Improvement of analysis models considering evolving vulnerability state, due to cascading and cumulative effects, through numerical simulations and experimental tests, possibly also supported by AI applications;
- Collected reliable data (same granularity and format) and ways to share and analyse it. The interoperability of all kinds of systems and information sharing is crucial, based on the need-to-know principle;
- Improved knowledge/experience-sharing from past emergencies to cope with future emergencies, also strengthening trans-national knowledge and data exchange among EU countries as well as from early warning to early action;
- Improved disaster risk and resilience management due to single/multiple threats through a holistic, systemic and cross-cutting approach, also considering relevant changes such as changing climate, digital transformation, environmental and socio-economic conditions;
- Development of holistic Risk and Resilience Metrics to support multi-hazard prevention strategies, encompassing main physical, economic and social effects;
- Solutions shall include the analysis of the physical, social and governance systems and take into account the development of an EU comprehensive risks and threats assessment.

[119] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Scope: Advancing multi-hazard risk assessment and disaster resilience is a necessity. Building on the integrated all-hazard approach, the advancement will be achieved by integrating single-hazard models into next-generation predictive systems capable of analysing cascading and cumulative effects. A key focus should be on early and anticipatory action, improving the understanding of interactions between meteorological, geophysical, and technological hazards, including their compounding impacts on societies, economies, and critical infrastructure.

Proposals should aim to develop and validate integrated forecasting models, that enhance the prediction and management of multi-hazard scenarios, supports flexibility and extensibility, and coordination of responses by incorporating real-time data, AI-driven analytics, and remote sensing technologies. These models should facilitate improved hazard forecasting by addressing challenges in platform interoperability and data exchange, ensuring that diverse hazard monitoring systems at local, national, and global levels can effectively communicate and operate in synergy.

Efforts should also explore the interoperability of regional and national hazard warning systems, enhancing global forecasting capabilities for hazards such as landslides triggered by extreme weather events, or cumulative damage modelling for earthquakes and their aftershocks. Research should address gaps in loss estimation models by considering the cascading and long-term impacts of disasters on infrastructure, the built environment, supply chains, and diverse needs of communities. Furthermore, proposals should contribute to the development of advanced tools and methodologies to assess the combined effects of multiple hazards on critical infrastructure, ensuring that disaster risk management strategies account for interdependencies across sectors This should include scenario-based stress testing, digital twins for risk modelling, and AI-powered decision-support systems, taking into account existing biases, to enhance resilience planning for lifeline services such as energy, water, transport and telecommunications.

A holistic, systemic, and cross-cutting approach should be applied to disaster risk management, taking into consideration climate change trends, environmental degradation, and vulnerabilities such as gender, age, disabilities and others social factors. The topic should lead to the creation of comprehensive Risk and Resilience Metrics, integrating physical, economic, and social dimensions to support decision-makers in designing effective prevention and adaptation strategies. Considering building on and leveraging from existing systems, such as the Copernicus Emergency Management Service (CEMS) the Destination Earth Platform or Risk Data Hub, could be beneficial.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities.

Projects may take into account the assets but also particular challenges faced by the European outermost regions and may include entities from these regions in the consortium’s composition.

Projects should contribute to strengthening risk governance at multiple levels by fostering collaboration between scientific communities, policymakers, emergency responders, and infrastructure operators. Efforts should be made in leveraging citizens-generated content in social media and decentralised digital platforms for citizen-driven early warning and situational awareness. Alignment with EU policies, international risk reduction frameworks, and best practices in resilience planning should be ensured, maximizing the applicability and impact of the developed solutions. The Preparedness Union Strategy is a key document in this regard and includes a key action on developing an EU comprehensive risks and threats assessment. Finding synergies with projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[120], is recommended.

Where applicable, proposals should leverage the data and services available through European Research Infrastructures federated under the European Open Science Cloud, as well as data from relevant Data Spaces. Particular efforts should be made to ensure that the data produced in the context of this topic is FAIR (Findable, Accessible, Interoperable and Re-usable).

**HORIZON-CL3-2026-01-DRS-03: Development of innovative tools, processes, equipment and technologies through responses to disasters and emergencies for search and rescue in hazardous conditions**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks. |

120 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

| | |
|---|---|
| | Due to the scope of this topic, relevant international organisations with headquarters in a Member State or Horizon Europe Associated Country are exceptionally eligible for funding.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 practitioner organisations (first responders) and 2 medical emergency authorities from at least 3 different EU Member States or Associated Countries.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [121]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

[121] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Creation of cutting-edge tools, processes, equipment and technologies to enhance disaster and emergency response capabilities for various practitioners as well as for assets, such as vehicles, aircraft, and heavy equipment;

- Taking into consideration existing technologies, development of autonomous drones, robotics, and other technologies specifically designed for emergency medical response and search and rescue operations in hazardous conditions such as wildfires, earthquakes and large-scale events;

- Improvement of response efficiency and safety for survivors and emergency practitioners through the adoption of advanced, technology-driven solutions in disaster scenarios;

- Consider needs of existing EU-level capacities, emergency reserves, and stockpiling in the deployment of the assets and being able to move them.

Scope: The scope of this topic is the development of innovative tools, equipment, and technologies to enhance the capabilities of emergency responders operating in complex and hazardous disaster environments. By leveraging advancements in smart protective equipment, in robotics, autonomous systems, remote sensing, communication and human sensor technologies, the aim is to improve the efficiency, safety, and effectiveness of emergency medical response and search and rescue operations, particularly in high-risk scenarios, such as wildfires, earthquakes and large-scale trauma events.

Proposals should explore the design, testing, and validation of innovative solutions capable of performing critical tasks in disaster-stricken areas. These technologies should be tailored to operate in extreme conditions, including high temperatures, unstable terrains, and low-visibility environments and beneficial to all individuals regardless of their age, gender or ability. Research should address challenges related to autonomous navigation, AI-driven decision-making, real-time situational awareness, and seamless integration with existing command-and-control systems used by disaster management. Collaboration of different practitioners should be supported to support proper market uptake.

Efforts should be made to enhance interoperability and data-sharing capabilities between various platforms, emergency response teams, and crisis management systems. A key aspect of this research should be the practical deployment and validation of these technologies through field exercises and simulations in real-world disaster scenarios. User-driven design approaches, prioritising inclusivity and accessibilities should ensure that developed solutions align with the operational needs of responders in disasters., Proposals should develop a command-and-control solution that allows organisation of all activities, ensuring a swift, coordinated, and effective response to any disaster with clear plan for uptake after the project.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and the relevant authorities. The current response capacities of the

European Civil Protection Pool[122] its capacity gaps[123], and the rescEU strategic reserve[124] as well as the EU Stockpiling Strategy should be taken into account in the roadmap to ensure needs-based approach. Thus, the proposals could consider innovation for heavier assets, such as flood containment and high-capacity pumping, transport or response aircraft, shelters and power generators, ground firefighting vehicles and aerial firefighting helicopters.

Furthermore, proposals should consider ethical, legal, and social implications associated with the deployment of autonomous technologies in emergency response. Issues such as data privacy, cybersecurity, human- and animal life protection, public acceptance, and compliance with regulatory frameworks should be addressed to facilitate the responsible and effective use of these innovations.

Projects should contribute to strengthening Europe's disaster response capacity by equipping practitioners with state-of-the-art technological solutions that enhance their ability to operate safely and efficiently in life-threatening environments. Alignment with EU policies and international best practices should be ensured to maximize the scalability and real-world applicability of the developed solutions. The Preparedness Union Strategy is a key document in this regard. Finding synergies with projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[125], is recommended.

**HORIZON-CL3-2026-01-DRS-04: Open topic on driving innovation uptake of disaster risk solutions**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are |

122 https://civil-protection-knowledge-network.europa.eu/media/ecpp-capacities-brochure
123 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0286
124 https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/resceu_en
125 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

| | |
|---|---|
| | directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 first responders or authorities in charge of disaster risk[126] from at least 3 different EU Member States or Associated Countries.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [127]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU |

[126] Authorities in charge of disaster risk entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement disaster risk prevention, preparedness, or response, measures.

[127] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| | classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Accelerated adoption of high-TRL (Technology Readiness Level) disaster risk solutions across diverse sectors;
- Facilitated integration of innovative technologies into existing disaster prevention, preparedness, response, and recovery frameworks;
- Promoted collaboration among stakeholders to scale proven solutions and enhance resilience;
- Addressed barriers to deployment, ensuring accessibility and usability of advanced DRS technologies;
- Strengthened evidence-based decision-making through demonstration and validation of high-TRL solutions in real-world scenarios;
- Promoted visibility of civil security research results.

Scope: This topic aims to foster the widespread adoption and integration of high-TRL (Technology Readiness Level) disaster risk solutions (DRS) across multiple sectors, enhancing societal resilience to various hazards, including climate. The focus is on overcoming barriers to deployment, ensuring accessibility, and strengthening collaboration among stakeholders to drive innovation uptake. Projects should promote the adoption of high-TRL solutions by public and private sector organizations involved in disaster risk management, developing strategies for scaling and commercializing innovative DRS technologies to ensure they reach end-users efficiently. They should also demonstrate how these technologies can complement or replace existing disaster preparedness, response, and recovery frameworks by developing integrated governance and coordination models across sectors and levels for disaster preparedness, response, and recovery in multi-hazard and cascading risk scenario interoperability standards, and guidelines for integrating new solutions into national and European civil protection systems. The project should especially liaise and support other disaster resilience projects in driving their uptake as well as examine how to build synergy pathways with other preparedness grants, such as Knowledge for Action in Prevention & Preparedness (KAPP) funding call of the Union Civil Protection Mechanism (UCPM).

Addressing deployment barriers is crucial, including identifying and mitigating technical, regulatory, financial, and social obstacles hindering the uptake of advanced solutions, while ensuring accessibility and usability for diverse stakeholders such as first responders, local authorities, and communities and individuals in a vulnerable situation. Projects should also demonstrate the real-world effectiveness of high-TRL solutions through large-scale pilot projects and demonstrations, generating robust evidence to support data-driven decision-

making and optimize disaster risk reduction strategies. Initiatives should consider the capacity gaps of the UCPM[128], align with EU disaster resilience objectives and build on existing programs, ensuring synergies with relevant policies, funding mechanisms, and technological ecosystems. The private-public cooperation chapter of the Preparedness Union Strategy should especially be a guiding document. Proposals are encouraged to incorporate digital tools, AI-driven analytics, digital twins such as Destination Earth, IoT applications, and other emerging technologies to enhance disaster preparedness and response.

Proposals should have a strategy to promote the visibility of the project and the results to the broader public in order to show the potential of European civil security research (political sphere, private sector, citizens). This could entail the European Civil Protection Forum and the European Commission Disaster Risk Management Knowledge Centre platform as examples.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

**HORIZON-CL3-2026-01-DRS-05: Climate security and civil preparedness – new ways to develop pre- and post-crisis climate-change related scenarios for a more resilient Europe**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 4.50 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The Joint Research Centre (JRC) may participate as member of the consortium selected for funding as a beneficiary with zero funding, or as an associated partner. The JRC will not participate in the preparation and submission of the proposal - see General Annex B.<br>Due to the scope of this topic, relevant international organisations with headquarters in a Member State or Horizon Europe Associated Country are exceptionally eligible for funding. |

128 eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0286

| | |
|---|---|
| | The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 authorities in charge of disaster risk[129] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [130]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

[129] Authorities in charge of disaster risk entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement disaster risk prevention, preparedness, or response, measures.

[130] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Identification and prioritization of climate security scenarios, assessing cascading and compounding risks across multiple sectors;
- Development and validation of advanced tools, technologies, and data-driven solutions for climate - and environmental - risk forecasting, crisis management, and adaptation, including risk analytical and assessment tools, weather alerts and forecasts;
- Development and validation of advanced tools and technologies to assess and monitor climate-induced disasters, also providing risk information on adaptation and risk reduction measures;
- Strengthened engagement with stakeholders, ensuring end-user involvement in defining requirements, testing, and validation of climate security solutions;
- Development and validation of new risk-management tools, technologies and data, closer to operational environment. Focus on local and regional risk-management and climate adaptation work should be prioritized;
- Pre-crisis analysis and post-crisis situational awareness in case of those disasters related to climate change (floods, fires, landslides, heat waves, etc.);
- Enhanced international cooperation, policy integration, and public awareness to improve climate security resilience and preparedness. Strengthen networks to exchange best practices and support the international dimension of the Preparedness Union Strategy and the Sendai Disaster Risk Reduction Framework.

Scope: Climate change is a global challenge with profound security implications at the global, regional, and local levels. It exacerbates risks across multiple sectors, including agriculture, biodiversity, health, border security, economy, financial stability, transport, telecommunication and human displacement, leading to severe socio-economic consequences and destabilizing communities. The increasing frequency and intensity of climate-related disasters highlight the urgent need for a holistic, long-term strategy to address climate security, integrating risk assessment, crisis management, and adaptation measures, while also leveraging the expertise of the insurance sector.

While climate services based on data analysis have reached a high level of trust among users, their application to civil security remains underdeveloped. Proposals should aim to develop methodologies, tools, and technologies that enhance situational awareness both before a crisis (pre-crisis) and after a crisis (post-crisis), enabling decision-makers and populations to respond effectively. Research should focus on defining priority climate security scenarios in the EU, identifying key stakeholders, and establishing essential indicators for informed decision-making.

Efforts should be directed toward understanding and mitigating the impacts of floods, landslides, wildfires, and other climate-induced disasters. This includes developing improved methods and models for risk prevention and reduction, early detection, emergency response tactics, and rescue efforts under extreme conditions. The study of cascading effects and

compounding disasters is critical, particularly regarding groups in a vulnerable situation such as older people, people with disabilities, and children. In this view, the proposals should build on the European Climate Risk Assessment (EUCRA[131]) and consolidated national risk assessments[132] as well as find synergies with project's chosen for the similar EU Mission: Adaptation to Climate Change topic[133]. Both the European Preparedness Union Strategy, the European Water Resilience Strategy and the upcoming European Climate Adaptation Plan act as policy guidance.

Diverse climate and environmental security scenarios should be developed, supported by innovative, reliable tools that leverage multiple data sources, enabling a comprehensive and adaptive response. Proposals should also integrate space programme components such as Copernicus and Galileo to improve data accuracy and crisis response capabilities. A strong emphasis on international cooperation should foster knowledge exchange, enhance policy integration, and share best practices. Proposals should support transnational collaboration within the EU, facilitate improved data-sharing mechanisms, and align with global initiatives such as the Sendai Disaster Risk Reduction Framework. Capacity-building efforts to strengthen resilience to climate-related security threats and ensure a coordinated approach to addressing worst-case climate scenarios, as identified in the Niinistö report[134].

Projects may take into account the assets but also particular challenges faced by the European outermost regions and may include entities from these regions in the consortium's composition.

Where applicable, proposals should leverage the data and services available through European Research Infrastructures federated under the European Open Science Cloud, Copernicus, Destination Earth, as well as data from relevant Data Spaces. Particular efforts should be made to ensure that the data produced in the context of this topic is FAIR (Findable, Accessible, Interoperable and Re-usable).

Where relevant, funded projects are encouraged to liaise with the European Commission's Joint Research Centre, for complementary real-scale testing at the Reaction Wall and HopLab of the European Laboratory for Structural Assessment (ELSA).

**HORIZON-CL3-2027-01-DRS-01: Open Topic on advanced protective gear optimized for CBRN-E (Chemical, Biological, Radiological, Nuclear, Explosives) environments and new generation of smart protective equipment for disaster responders**

| **Call: Civil Security for Society 2027** |
|---|
| **Specific conditions** |

131 https://www.eea.europa.eu/en/analysis/publications/european-climate-risk-assessment

132 COM/2024/130 final, Preventing and managing disaster risk in Europe, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0130

133 HORIZON-MISS-2026-01-CLIMA-04: Bridging the gap between disaster risk management and climate adaptation

134 https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en

| | |
|---|---|
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.835 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 7.67 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of:<br>• at least 2 Training Centres[135] located in EU Member States or Associated Countries, and<br>• at least 2 practitioners involved in training, validation and testing of CBRN-E tools and technologies from at least 2 EU Member States or Associated Countries.<br>For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the |

[135] Training centres are national, regional or local infrastructures, generally ruled by governments or professional organisations, aiming at training practitioners (first responders, civil protection units etc.) in near-real operational crisis situations.

| | |
|---|---|
| | Research and Training Programme of the European Atomic Energy Community (2021-2025) [136]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Developed of advanced protective gear specifically designed for optimal performance in Chemical or Biological or Radiological, and Nuclear or Explosives (CBRN-E) environments;
- Created innovative smart protective equipment for disaster responders, incorporating advanced technologies to enhance safety and operational efficiency;
- Improvement of protective solutions to ensure the safety and effectiveness of disaster responders operating in hazardous and high-risk environments.

Scope: This topic aims to advance the development of protective gear specifically designed for optimal performance in specificities of the Chemical, Biological, Radiological, Nuclear, and Explosives (CBRN-E) environments, along with the creation of a new generation of smart protective equipment for disaster responders. Projects should focus on the use of innovative materials, technologies, and design features that enhance the protective capabilities of gear used in high-risk, hazardous environments, ensuring the safety and well-being of disaster responders_with an inclusive and user-centric approach. The integration of advanced technologies will be crucial to enhancing the operational efficiency and effectiveness of the equipment.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities. The current response capacities of the European Civil Protection Pool[137] and the rescEU strategic reserve[138] should be taken into account in the roadmap to ensure needs-based approach.

Proposals should build upon existing research outputs, specifically under other Horizon Europe Cluster 4, and technologies to create smart, adaptive protective solutions that respond dynamically to evolving threats in CBRN-E scenarios. This includes the incorporation of features similar to automated hazard detection, environmental monitoring, and advanced

[136] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

[137] https://civil-protection-knowledge-network.europa.eu/media/ecpp-capacities-brochure

[138] https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/resceu_en

communication systems to provide real-time situational awareness. The new gear should meet rigorous safety standards while improving the comfort, mobility, and usability of responders, enabling better performance and faster decision-making in demanding environments.

Proposals should focus on providing comprehensive solutions that combine robust protection, operational support, and data-driven insights, ensuring a holistic approach to safety. Collaboration between research institutions, manufacturers, and end-users will be essential to ensure that the resulting products meet the practical requirements of practitioners in the field. The Preparedness Union Strategy is a key document in this regard. Analysing the capacity gaps of the UCPM[139] as well as finding synergies with the rescEU strategic reserve and projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[140], is recommended.

**HORIZON-CL3-2027-01-DRS-02: Societal resilience, engagement of the younger generations and digital innovation for disaster resilience**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 6.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 Civil Society Organisation (CSO) and 2 NGOs representing young people or youth organisations from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all the requested information, following the template provided in the submission IT tool. |

139 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0286

140 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

| | |
|---|---|
| | If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [141]. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Developed a tailored education programs for younger generations, incorporating digital tools and gamification to enhance disaster awareness and engagement;
- Strengthened societal resilience by actively involving younger generations, citizens, and local authorities in disaster preparedness and response initiatives;
- Promoted collaborative research that integrates youth perspectives and community involvement, fostering a more resilient society in the face of disasters and crises;
- Enhanced resilience and behaviour of children, young people, and other groups in a vulnerable situation before, during, and after climate-related disasters and health emergencies;
- Training and education tools to engage young people and other populations a vulnerable situation in preparedness and crisis management.

Scope: This topic focuses on enhancing societal resilience by actively engaging younger generations in disaster preparedness, response, and recovery through digital innovation, education, and community involvement. Projects should develop tailored innovative solutions

[141] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

that integrate digital tools, gamification, and interactive learning methods to improve disaster awareness, risk perception, and response capabilities among younger generations. These initiatives should empower younger generations [142], to become active contributors to resilience-building efforts, equipping them with the knowledge and leadership skills.

Particular attention should be given to the behaviour of children, young people, and other groups in a vulnerable situation before, during, and after climate-related disasters and health emergencies. Participatory approaches, including youth-led initiatives, citizen science, and digital engagement platforms, should be prioritized to enhance community-based resilience and ensure young people's perspectives are integrated into decision-making processes. These approaches should follow an intersectional approach that gives credit to the (growing) heterogeneity of young people. Best practices from other programmes should be taken into account.

Proposals should also focus on leveraging emerging technologies - such as artificial intelligence, virtual and augmented reality, social media analytics, and serious games - to engage young people in disaster preparedness and crisis response. Additionally, innovative communication strategies should be explored to enhance youth participation, particularly through digital technologies and social media. Practical examples, including pilots and real-world case studies, should be developed to test and refine these approaches.

Proposals should explore methods to interconnect young people's data with crisis management teams, practitioners, and authorities, ensuring that their contributions are effectively integrated into emergency response frameworks. Training and education tools should be designed to engage young people and other vulnerable populations in preparedness and crisis management, promoting long-term resilience.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities.

The support and involvement of citizens and civil society is central to achieving the targeted outcomes.

By fostering collaborative research and youth-driven initiatives, projects should contribute to innovative and inclusive resilience strategies that align with EU policies on disaster risk reduction, education, digital transformation, and civil protection. Proposals should ensure synergies with existing initiatives and frameworks, such as the Preparedness Union Strategy's chapter on population preparedness, Erasmus+ and the European Solidarity Corps, as well as the Sendai Disaster Risk Reduction Framework. Finding synergies with projects from

[142] In the context of the European Union, youth is typically defined as individuals between the ages of 13 and 30. This definition aligns with the EU's Youth Strategy, which focuses on supporting young people's personal and professional development. However, some EU programs may adjust the age range slightly depending on the specific context (e.g., education, employment, or participation), but the 13-30 age bracket is recognized in EU policies related to youth.

operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[143], is recommend.

**HORIZON-CL3-2027-01-DRS-03: Enhancing decision support system for disaster crises: leveraging emerging technologies for improved civil preparedness and crisis management**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 9.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 authorities in charge of disaster risk or crisis communication[144] and 2 representatives of local or regional authorities in charge of disaster response, from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the |

143 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

144 Authorities in charge of disaster risk and crisis communication entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement disaster risk prevention, preparedness, response or crisis communication measures.

| | |
|---|---|
| | submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [145]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of decision support systems for disaster crises, utilizing near real-time data from the ground to enhance situational awareness and response;
- Creation of systems designed to bolster civil preparedness, that enhance operational efficiency and response times, ensuring timely and effective management of various disaster scenarios including from early warning to early action
- Integration of advanced data analysis and decision-making tools to support authorities and first responders in disaster situations.

Scope: This topic focuses on enhancing existing decision support systems for disaster crises by integrating emerging technologies to improve civil preparedness and crisis management.

[145] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

The objective is to advance the capabilities of existing systems, making them more reliable, adaptable, and efficient through the incorporation of trustworthy AI technologies that ensure transparency, accountability, and ethical decision-making processes. Projects should aim to enable quicker and more informed responses during disaster scenarios.

Proposals should focus on creating advanced systems designed to strengthen civil preparedness, helping authorities and responders manage various disaster situations in a timely and effective manner. These systems should leverage cutting-edge AI-driven tools to process large volumes of data, providing actionable insights that improve decision-making during critical moments, such as from early warning to early action. Emphasis should be placed on integrating advanced data analysis and predictive modelling to anticipate disaster developments and guide interventions, while ensuring that the systems are transparent, explainable, and built on principles of trustworthiness, inclusive and gender sensitive and ethical AI use and on secure AI deployments.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities.

Additionally, test centres should play a key role in this research by increasing their capacity to trial and validate emerging technologies, supporting more effective civil preparedness and crisis response capabilities.

The expected outcome is to create systems that not only enhance operational efficiency and response times but also foster better collaboration among stakeholders, including local authorities, emergency services, and other relevant actors. This includes integrating drones with state emergency vehicles, smart traffic systems, and law enforcement to enhance data driven disaster preparedness and emergency response, ensuring effective coordination and faster decision-making for local authorities.

Projects should also contribute to improving the usability and accessibility of decision-support systems for diverse users, ensuring they are easily integrated into disaster management frameworks and can be used effectively in different crisis situations. The solutions should align with EU guidelines on AI ethics[146] and resilience-building, ensuring they complement existing civil protection and crisis management initiatives while driving innovation in disaster risk reduction. The Preparedness Union Strategy is a key document in this regard. Analysing the capacity gaps of the UCPM[147] and finding synergies with projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[148], is recommended.

146 AI Act: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

147 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0286

148 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Where applicable, proposals should leverage the data and services available through European Research Infrastructures federated under the European Open Science Cloud, Copernicus, Destination Earth as well as data from relevant Data Spaces. Particular efforts should be made to ensure that the data produced in the context of this topic is FAIR (Findable, Accessible, Interoperable and Re-usable).

**HORIZON-CL3-2027-01-DRS-04: Enhancing preparedness for large-scale cross-border disasters**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 8.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>Due to the scope of this topic, relevant international organisations with headquarters in a Member State or Horizon Europe Associated Country are exceptionally eligible for funding.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 authorities in charge of disaster risk or crisis communication[149], from at |

[149] Authorities in charge of disaster risk or crisis communication entail public bodies operating at the national level that hold legally defined responsibilities in the area of disaster risk management. This includes national civil protection authorities as well as other institutions that can demonstrate, through

| | |
|---|---|
| | least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [150]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Utilization of virtual and augmented reality training to simulate large-scale and transboundary disasters, improving disaster management's readiness and response capabilities;
- Development of diverse crisis scenarios using VR/AR technology, providing immersive, practical training experiences for emergency personnel, responders and decision makers;

appropriate legal or administrative acts, a formal mandate to design, coordinate, or implement disaster risk prevention, preparedness, response or crisis communication measures.

150 This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Strengthened ability of responders and decision-makers to manage large-scale, cross-border disaster scenarios through advanced, technology-driven training programs;

- Improved knowledge/experience-sharing from past emergencies to cope with future emergencies, also strengthening trans-national knowledge and data exchange among EU countries as well as from early warning to early action.

Scope: The scope of this topic is on enhancing preparedness for large-scale, cross-border disasters by leveraging advanced training methodologies, including virtual reality (VR) and augmented reality (AR) simulations and Digital Twins. The objective is to improve the readiness and response capabilities of disaster responders and emergency management personnel by providing immersive, technology-driven training experiences that replicate complex disaster scenarios.

Proposals should develop and validate innovative VR/AR-based crisis simulation models that can accurately depict diverse large-scale disaster situations, including transboundary hazards such as wildfires, floods, earthquakes, and industrial accidents. These simulations should incorporate near real-time data, AI-driven scenario adaptation, and multi-user interaction capabilities to ensure realistic, high-impact training exercises. Special attention should be given to the interoperability of these training platforms, allowing emergency services from different regions and countries to collaborate in joint preparedness exercises. Recommendations taken into account a gender-sensitive approaches should also improve crisis simulations by considering diverse needs and experiences.

Research should also explore how digital training environments can enhance situational awareness, decision-making, and coordination among disaster management and relevant authorities. The integration of gamification techniques, AI-driven coaching systems, and real-time performance assessment should be considered to maximize learning outcomes and adaptation to evolving crisis scenarios linking to previous themes (e.g. biometrics and long-lasting disturbance, or whole of the society security, multi-hazard theme etc.).

Furthermore, proposals should focus on strengthening knowledge and experience-sharing mechanisms across EU member states by developing transnational training frameworks and crisis management protocols, in coordination with the UCPM Training Programme[151]. This should include the establishment of digital platforms and collaborative networks to facilitate the exchange of lessons learned from past emergencies, fostering continuous improvement in disaster response strategies.

Projects should conduct a stakeholder or market analysis and a roadmap or plan for uptake of the developed methodologies, findings, and technologies to the industry, the research and innovation community, and/or the relevant authorities.

Ethical, legal, and social aspects related to the use of immersive training technologies should also be addressed, ensuring compliance with data protection regulations and maximizing public trust in the adoption of these tools. Trust should also refer to the security of the tools,

[151] https://civil-protection-knowledge-network.europa.eu/UCPM-training-programme

that should include appropriate measures for resilience against emerging cryptographic threats. Projects should align with existing EU disaster risk reduction policies and international best practices to ensure the practical applicability and scalability of the developed solutions. The Preparedness Union Strategy is a key document in this regard. Its key action on "Develop an EU catalogue for training and a platform for lessons learned" and existing platforms should be taken into account in the proposal. Analysing capacity gaps of the UCPM [152] and finding synergies with projects from operational grants, such as the Knowledge for Action in Prevention & Preparedness (KAPP)[153], is recommended.

Where applicable, proposals should leverage the data and services available through European Research Infrastructures federated under the European Open Science Cloud, Copernicus, Destination Earth as well as data from relevant Data Spaces. Particular efforts should be made to ensure that the data produced in the context of this topic is FAIR (Findable, Accessible, Interoperable and Re-usable).



152 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0286

153 Knowledge for Action in Prevention and Preparedness (KAPP) - European Commission - https://civil-protection-humanitarian-aid.ec.europa.eu/funding-evaluations/financing-civil-protection/cp-calls-proposals/knowledge-action-prevention-and-preparedness-kapp-0_en

**Destination - Strengthened Security Research and Innovation**

Since the Preparatory Action for Security Research[154] the EU-funded security research and innovation programme has contributed substantially to knowledge and value creation in the field of internal security. The programme has been fundamental to the consolidation of a European security ecosystem, which is better equipped to capitalise on research and innovation outcomes to support the EU security priorities. This Destination aims to contribute to reducing thematic fragmentation, bringing closer together the actors from different security domains, and expanding the market beyond traditional thematic silos. It also creates knowledge and value through research in matters (including technology, but also social sciences and humanities) that are not exclusive of only one security area, but cross-cutting to the whole Cluster.

As underlined in the Horizon Europe strategic plan 2025-2027, proposals for the topics under this Destination *'should support with cross-cutting actions the expected impacts outlined above [in the Cluster 3 Destinations]. This destination will increase the impact of the work carried out in the EU security Research and Innovation (R&I) ecosystem and contribute to its core values, namely:*

- *a focus on the potential and practical final use of the outcomes of security R&I;*
- *forward-looking planning of EU security capabilities;*
- *the development of security technologies that are socially acceptable, developed in quadruple helix*[155] *and that have added value for industrialisation, joint procurement, commercialisation, and the acquisition and deployment of successful R&I outcomes;*
- *safeguarding the EU's open strategic autonomy and technological sovereignty in critical security areas by contributing to a more competitive and resilient EU civil security technology and industrial base;*
- *experimenting with research and innovation programming; and*
- *helping to make the European R&I ecosystem more consistent'.*

Many of the programme outcomes have materialised in relevant scientific findings, maturation of promising technology areas, operational validation of innovative concepts or support to policy implementation. However, a key challenge remains in improving innovation uptake and thus contributing to the development of security capabilities[156], support of Start-

154 COM(2004) 72.

155 *Through the interaction of public authorities, academia, industry and the public.*

156 For the purpose of the work programme, the terms "Capability" should be understood as "the ability to pursue a particular policy priority or achieve a desired operational effect". The term "capability" is often interchanged with the term "capacity", but this should be avoided. "Capacity" could refer to an amount or volume of which one organisation could have enough or not. On the other hand, "capability" refers to an ability, an aptitude or a process that can be developed or improved in consonance with the ultimate objective of the organisation.

ups and Small-Medium Enterprises (SMEs) and deployment of innovation by security practitioners.

The extent to which innovative technologies developed thanks to EU R&I investment are industrialised and commercialised by EU industry, and acquired and deployed by end-users, could reflect the impact achieved with the programme. As explained in the Commission staff working document on Enhancing security through research and innovation[157] there are factors inherent to the EU security ecosystem (often attributed to the market) that hinder the full achievement of this impact, such as market fragmentation, cultural barriers, analytical weaknesses, programming weaknesses, ethical, legal and societal considerations or lack of synergies between funding instruments, among others. To that aim, there is a need to create a favourable environment that is designed with the main purpose of increasing the impact of security R&I, which provides the right tools that serve to tackle the factors that hinder innovation uptake.

Therefore, security research and innovation should foster and enhance the development of innovative tools, technologies and capabilities for the benefit of practitioners that can use in their day-to-day work. To this end, proposals under this Destination should set out a credible pathway to contributing to the following impacts:

- A more effective and efficient evidence and knowledge-based development of EU civil security capabilities built on a stronger, more systematic and analysis-intensive security research and innovation cycle;
- Increased cooperation between demand and supply market actors, including with actors from other domains, fosters swift industrialisation, commercialisation, adoption and deployment of successful outcomes of security research and reinforces the competitiveness and resilience of EU security technology and industrial base and safeguards the security of supply of EU-products in critical security areas;
- R&I-enabled knowledge and value in cross-cutting matters reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions.

This Destination will trigger actions that will help bringing these and other developments closer to the market, thus contributing to the measures facilitating the uptake of innovation. Those actions will help developers (including industry, research organisations and academia) to accelerate product development and improve the valorisation of their research investment. They will also support buyers and users in materialising the uptake of innovation and further develop their security capabilities. The aim is to increase the capacity of EU public procurers to align their requirements with the EU security industrial capacity and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

157 https://home-affairs.ec.europa.eu/document/download/ff888398-0b0a-4511-9717-ad41beb22314_en?filename=SWD-2021-422_en.PDF

Finally, this Destination will contribute to the development of the tailored analytical capacity required for the adoption of capability-driven approaches aimed at fostering a forward-looking capability-driven approach in security.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS)[158] activities and/or other international events.

Legal entities established in China are not eligible to participate in both Research and Innovation Actions (RIAs) and Innovation Actions (IAs) falling under this destination. For additional information please see "Restrictions on the participation of legal entities established in China" found in General Annex B of the General Annexes.

Proposals are invited against the following topic(s):

**HORIZON-CL3-2026-01-SSRI-01: Open topic on supporting disruptive technological innovations for civil security**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 2 relevant practitioners and 1 Research and Technology Organisation (RTO). For participants with practitioner status, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. |

158 https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

| | |
|---|---|
| | If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [159]. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved preparedness, evidence-based approaches and response capabilities, along with a strengthened ability to mitigate risks from diverse threats, by integrating validated disruptive technologies into real-world operations;
- Accelerated adoption of innovative solutions by reducing barriers through rigorous testing and validation, fostering collaboration among public authorities, industry, and researchers to align technologies with real-world needs.

Scope: This topic aims to support the integration of disruptive technological innovations[160] into civil security by strengthening research and innovation activities that enhance preparedness, response capabilities, and risk mitigation. A key focus is bridging the gap

159 This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

160 In the context of this Destination, the concept of 'disruptive technological innovations' refers to breakthrough technologies starting at low or very low TRL (<4) and holding the promise of inducing a paradigm shift in the way civil security operations are currently carried out, e.g. by significantly improving performance and/or reducing costs if further developed.

between early-stage, low Technology Readiness Level (TRL) research and applied security solutions, ensuring that emerging technologies are effectively transitioned into operational use.

Proposals should prioritize disruptive solutions that address diverse security threats while improving the efficiency and effectiveness of civil security operations. Emphasis should be placed on ensuring that these technologies are robust, reliable, scalable, and aligned with the needs of security practitioners. This includes fostering a structured pathway for transitioning low TRL innovations into practical applications, ensuring rigorous testing and validation processes for safety, performance, and interoperability.

To achieve this, proposals should promote strong collaboration between researchers, public authorities, industry partners, and end-users. Such partnerships will help align technological advancements with real-world security needs, facilitating the co-development of solutions that are both innovative and operationally relevant. Ensuring that emerging technologies are ethically sound, transparent, and accessible will also be crucial to their successful adoption.

The expected outcomes of this topic include improved preparedness through the adoption of cutting-edge technologies tailored to emerging security challenges, enhanced risk mitigation capabilities, and the accelerated integration of disruptive innovations into civil security frameworks. By fostering a collaborative ecosystem, projects should ensure that promising research transitions effectively into practical security applications, contributing to a more resilient and adaptive civil security landscape across Europe.

To ensure that the proposed research and innovation activities are aligned to EU long-term strategic priorities, proposers are encouraged to consult relevant technology foresight exercises[161].

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2026-01-SSRI-02: Demand-led innovation in security**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 5.83 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 5.83 million. |

[161] See, for instance, Conte, N., Maleville, A. d., Favino, R., Garcia Monreal, E., Montanari, E. et al., *Emerging risks and opportunities for EU internal security stemming from new technologies*, Publications Office of the European Union, 2025, https://data.europa.eu/doi/10.2760/9617320

| | |
|---|---|
| *Type of Action* | Pre-commercial Procurement |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the participation[162], as beneficiaries, of at least 3 practitioners and 3 public procurers[163]. These beneficiaries must be from at least 3 different EU Member States or Associated Countries. One organisation can have the role of practitioner and public procurer simultaneously, both counting for the overall number of organisations required for eligibility. Among the public procurers[164], minimum two must be independent legal entities that are public procurers, each established in a different Member State or Associated Country and with at least one of them established in a Member State.<br>For participants with practitioner status, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>PCP/PPI procurement costs are eligible. |

162 See General Annexes page 12 on the Consortium Composition as regards Pre-commercial Procurement.

163 Under this topic, the participation is required of minimum three procurers as beneficiaries in the buyer's group for the PCP. The third procurer in the buyer's group can be a private procurer or an NGO that provides similar services of public interest as the public procurers.

164 Under this topic, the participation is required of minimum three procurers as beneficiaries in the buyer's group for the PCP, out of which minimum two must be independent legal entities that are public procurers, each established in a different Member State or Associated Country and with at least one of them established in a Member State. The third procurer in the buyer's group can be a private procurer or an NGO that provides similar services of public interest as the public procurers.

| | |
|---|---|
| | The specific conditions for actions with PCP/PPI procurements in section H of the General Annexes apply to grants funded under this topic.<br><br>Beneficiaries must ensure that the subcontracted work is performed in at least 3 Member States — unless otherwise approved by the granting authority.<br><br>Beneficiaries may provide financial support to third parties. The support to third parties can only be provided in the form of grants / prizes. The maximum amount to be granted to each third party is EUR 100 000 to provide financial incentives to final end-users that are not part of the consortium (e.g., citizens) to adopt the solutions, including costly hardware components. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- A community of EU civil security practitioners with common user/functional needs for innovative technology solutions is identified, supported by an industrial base, in particular SMEs and Startups, to access the public procurement market and scale up their business;
- Procurers facilitated the commercialisation of the innovative solutions developed by their successful suppliers by providing them with first customer references for the validation and first pilot deployment;
- Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes that meet the diverse needs of the EU user community, regardless of their gender, age and ability;
- Improved delineation of the EU market (including demand and supply) for innovative civil security systems that can articulate alternative options for uptake in function of different industrialisation needs, commercialisation needs, acquisition needs, deployment needs and additional funding needs (beyond R&I funding).

Scope: As past experience shows that pre-commercial procurement opens up the procurement market for startups and enables the public sector to address societal challenges more effectively, public procurers should make more strategic use of PCP. Applicants are invited to submit proposals for PCP action to acquire Research and Development (R&D) services and innovative civil security technology solutions.

Proposals should demonstrate interest from a broader community of potential buyers, beyond the direct beneficiaries, who share similar needs and are open to jointly adopting the solutions developed, provided they are proven mature and operationally viable. The proposals are expected to include an analysis of the state of the art and market landscape, aligning research

activities with identified needs and presenting a range of technical alternatives to address the challenge. Furthermore, to stimulate dialogue with the supply side, public procurers are required to organise proposals that should demonstrate sustainability of the action beyond the life of the project.

The proposals should build on the outcomes of CSA projects funded under previous Horizon Europe work programmes aimed at creating *Stronger grounds for pre-commercial procurement of innovative security technologies*. The proposals should provide clear evidence to justify and de-risk the PCP action, demonstrating that the identified challenge is significant and necessitates a PCP action to mature certain technologies and compare alternatives. It should be shown that a consolidated group of practitioners and procurers with shared needs and requirements is committed to the PCP process, enabling informed decisions on future joint procurement of innovative solutions. Activities covered should include cooperation with policymakers to reinforce the national policy frameworks and mobilise substantial additional national budgets for PCP and innovation procurement in general beyond the scope of the project. The tender process to be followed is described in Annex H.

Proposals should demonstrate commitment to exploiting project results beyond its conclusion, ensuring engagement with stakeholders and implementation of strategies for future uptake. Applicants should also clarify measures to ensure compliance with the principles of the EU Directive on public procurement, particularly those related to PCP. The required open market consultations should be completed in at least three EU Member States. Prior consultations conducted under previous CSA projects should be used, provided they ensured procurement viability and remain relevant to the current state of the art.

Involvement of procurement decision makers is recommendable to ensure that end solution(s) are adopted by public buyers, increasing the societal impact of the related research activities. Therefore, procurers should declare in the proposal their interest to pursue deployment of solutions resulting from the PCP in case the PCP delivers successful solutions and indicate whether they will:

- Procure successful solution(s) as part of the PCP.
- Launch a separate follow-up procurement after the PCP to buy such type of solutions.
- Adopt successful solutions without the need to procure them (e.g. in case of open-source solutions).
- Foresee financial or regulatory incentives for others to adopt successful solutions (e.g. in case the final end-users of the solutions are not the procurers but for example citizens).

In these four cases, the procurers can implement the project as a fast-track PCP[165]. In the first case, the procurers should foresee the budget in the proposal to purchase at least one solution during the PCP. In the second case, the procurers should include in the proposal a deliverable that prepares the follow-up procurement to purchase such type of solution(s) after the PCP. In

[165] See General Annex H of the Horizon Europe Work Programme.

the first and third case, the procurers should foresee sufficient time during the project to deploy and validate that the solutions function well after installation. In the fourth case, the procurers can use financial support to third parties to provide financial incentives to final end-users that are not part of the consortium (e.g. citizens) to adopt the solutions, including costly hardware components, with a maximum budget of EUR 100.000.

Applicants should propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalising the tendering documents package for a PCP call for tenders based on the technical input, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.

- Moreover, to ensure the sustainability and uptake of the developed solutions, proposals should outline clear plans for post-PCP activities. As outlined in the general annexes of the Horizon Europe Work Programme 2026-2027, the topic allows public buyers to use the fast-track PCP option (e.g. 2 instead of 3 phases) when they commit to buying or deploying the resulting solutions after the PCP. However, if such a commitment is not yet in place at the proposal stage, the call expects proposers to include a deliverable outlining concrete activities to prepare the ground for follow-up deployment or procurement after the PCP.

- Launching the call for tenders for research and development services. The call for tenders should envisage a competitive development composed of different phases that would lead to at least 2 prototypes from 2 different providers to be validated in real operational environment at the end of the PCP cycle;

- Conducting the competitive development of the prototypes following the PCP principles including a design phase, an integration and technical verification phase and a validation in real operational environment phase. In evaluating the proposals and the results of the PCP phases, the applicants should consider technical merit, feasibility and commercial potential of proposed research efforts.

- Consolidating the results of the evaluation of the developed prototypes, extracting conclusions and recommendations from the validation process, and defining a strategy for a potential uptake of solutions inspired in the PCP outcomes, including a complete technical specification of the envisaged solutions and standardisation needs and/or proposals. This strategy should consider joint-cross border procurement schemes and exploit synergies with other EU and national non-research funds.

Applicants are expected to maximise the visibility of the project outcomes to the wide community of potential EU public buyers. Liaison with other civil security communities beyond those addressed by the project is encouraged in order to assess the possible reuse and extensibility of the identified solutions to different domains.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2026-01-SSRI-03: Public procurement of innovation for security**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 2.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 2.00 million. |
| *Type of Action* | Public Procurement of Innovative Solutions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the participation[166], as beneficiaries, of at least 3 practitioners and 3 public procurers. These beneficiaries must be from at least 3 different EU Member States or Associated Countries. One organisation can have the role of practitioner and public procurer simultaneously, both counting for the overall number of organisations required for eligibility. Among the public procurers[167], minimum two must be independent legal entities that are public procurers, each established in a different Member State or Associated Country and with at least one of them established in a Member State.<br>For participants with practitioner status, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may |

[166] See General Annexes page 12 on the Consortium Composition as regards Public procurement of innovative solutions.

[167] Under this topic, the participation is required of minimum three procurers as beneficiaries in the buyer's group for the PPI. The third procurer in the buyer's group can be a private procurer or an NGO that provides similar services of public interest as the public procurers.

| | |
|---|---|
| | additionally be used). |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>PCP/PPI procurement costs are eligible.<br>The specific conditions for actions with PCP/PPI procurements in section H of the General Annexes apply to grants funded under this topic. |
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Last mile support to previous pre-commercial procurement (PCP) actions;
- Development and deployment of innovative security solutions to address emerging threats, including post-quantum cryptography to counter emerging quantum threats, improving the effectiveness and efficiency of public security services;
- Implementation of pilot projects and real-world testing, ensuring scalability and contributing to innovative security technologies.

Scope: This Public Procurement of Innovative Solutions (PPI) initiative aims to advance the adoption of innovative civil security solutions. The focus is on solutions that have been partially demonstrated on a small scale and are nearly or already available in small quantities but have not yet been widely adopted or produced at scale. These solutions should demonstrate a clear market potential and be new to the procurers, their market segment, or the internal EU market, and must be relevant to procurers across EU Member States and/or Associated Countries.

This PPI will specifically target innovative solutions that can address critical challenges in civil security and that are aligned with market readiness criteria. The solutions should meet requirements for sustainability (both operational and environmental), interoperability, adaptability, and be commercially viable while still holding residual market risks, such as not yet being produced in large quantities or at market-ready quality and pricing.

This initiative will focus on solutions that have already demonstrated partially successful results but require scaling, refinement, or deployment in new environments to meet mass-

market price/quality standards. This is in line with Horizon Europe's objective of fostering the early adoption of innovations that are critical to improving civil security across Europe[168].

In compliance with the requirements of the Horizon Europe Work Programme – General Annex H, this action will engage in open market consultations with potential tenderers and end-users to identify gaps between perceived procurement needs and current industry developments. Feedback from these consultations will inform the PPI tender specifications, ensuring that the PPI emphasizes the early adoption of innovative solutions rather than the procurement of fully mature or mass-market technologies. The market readiness of the solutions can be verified through conformity testing, certification, or quality labelling. The work will also involve establishing evaluation criteria based on best-value-for-money rather than solely on the lowest price, ensuring that innovations are assessed for both their technical performance and their potential to deliver long-term value.

The PPI contract notices will be published EU-wide, with offers evaluated on objective criteria, ensuring transparency and fairness in the selection process. Functional/performance-based specifications will be used to define the challenges and problems to be solved, rather than prescriptive solutions, and procurement will avoid any conflicts of interest. The distribution of Intellectual Property Rights (IPR) will be clearly outlined in the PPI call for tenders, in line with the objective of promoting fair and wide exploitation of the results.

The process to be followed for the preparation and publication of the open market consultation and call for tender is described in General Annex H.

By fostering the early adoption of innovative technologies, this PPI initiative will enable the European civil security sector to address emerging threats, while contributing to the EU's broader goals of technological sovereignty and market innovation. This will allow public authorities to remain at the forefront of addressing evolving risks and threats. The action will also catalyse innovation, drive competition, and significantly reduce the time needed to move from the initial concept to market.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2026-01-SSRI-04: Development of ecosystem and next-generation capabilities for a secured European Critical Communication System in civil security**

| **Call: Civil Security for Society 2026** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a |

[168] For more information see General Annex H of Horizon Europe Work Programme – Specific Conditions for Actions with PCP/PPI.

| | |
|---|---|
| | proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 3.00 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility criteria apply:<br>This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [169]. |

[169] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:

| | |
|---|---|
| *Security Sensitive Topics* | Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Creation of an integrated ecosystem for secure and resilient communication systems to support civil security operations across Europe;
- Advancement of next-generation capabilities, ensuring robust, scalable, and interoperable communication systems for critical civil security functions relevant for the future EU Critical Communication System (EUCCS).

Scope: The European Union Critical Communication System (EUCCS) is a flagship initiative aiming at gradual development of a unified, secure, and interoperable communication infrastructure to support critical public safety and civil security operations across Europe. Aims to provide law enforcement, first responders, emergency services, and other critical sectors with reliable, real-time communication capabilities, even in challenging or high-risk environments. This topic aims to streamline the creation of an integrated ecosystem for secure and resilient communication systems that support civil security operations across Europe. It aims to advance next-generation capabilities, ensuring robust, scalable, and interoperable communication systems tailored to the critical civil security functions that will be required for the future EUCCS, taking into consideration the ongoing migration of the EU towards post-quantum cryptography.

The action funded under this topic will develop secure communication devices and applications that meet the unique needs of practitioners across various disciplines. These solutions will go beyond current technologies, enabling specialized, ruggedized devices that support hands-free capabilities, including wearable sensors, haptics, and augmented reality to enhance situational awareness. Devices will be designed to ensure communication in environments lacking cellular infrastructure and will be built with high standards of security, including addressing cryptographic security via post-quantum cryptography, and trustworthiness while also ensuring an inclusive and gender-sensitive approach to meet the diverse needs of all users. The action funded under this topic should support relevant standardisation processes where possible.

The solutions should be mission-critical, offering high availability, resilience, data exchange and authentication both secured via state-of-the-art post-quantum cryptographic protocols, even in areas with limited or no commercial network coverage. They must be fully compatible with the EUCCS, leveraging 3GPP Mission Critical Services (MCX) and open APIs to create a versatile and interoperable ecosystem. By working closely with first responders and utilizing

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

open platforms, the project will ensure that the developed solutions address the specific operational needs of responders, facilitating effective cross-agency and pan-European collaboration.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2027-01-SSRI-01: Accelerating uptake through open proposals for advanced SME innovation**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 4.50 million. |
| *Type of Action* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In line with the "*restriction on control in innovation actions in critical technology areas*" delineated in General Annex B of the General Annexes, entities established in an eligible country but which are directly or indirectly controlled by China or by a legal entity established in China are not eligible to participate in the action.<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility conditions apply:<br>Consortia must include, as beneficiaries:<br>- A minimum of three (3) to a maximum of seven (7) partners.<br>- At least 2 SMEs[170] from 2 different Member States.<br>- At least 1 end-user organisation in the areas addressed by the proposal, namely one of the following options:<br>• Option A "Fighting Organised Crime and Terrorism'' |

[170] See Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises, as well as the User Guide for SME definition.

| | |
|---|---|
| | • Option B ‘"Disaster-Resilient Society’’<br>• Option C "Resilient Infrastructure’’ and<br>• Option D ‘"Border Management’’.<br>Participation of non-SME industries and Research and Technology Organisations (RTOs) is not excluded, but it must be limited to 15% of the proposed budget.<br>At least 50% of the proposed budget must be allocated to SMEs.<br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Procedure* | The procedure is described in General Annex F. The following exceptions apply:<br>Eligible proposals submitted under this topic and exceeding all the evaluation thresholds will be awarded a STEP Seal [https://strategic-technologies.europa.eu/about/step-seal_en]. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [171]. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of a mature technological solution addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme and in particular the destination

[171] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under ‘Simplified costs decisions’ or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

of fighting crime and terrorism, disaster resilient societies, border management and resilient infrastructure;

- Facilitate increased and sustained collaboration between small and medium-sized enterprises (SMEs), public research partners, and academia, leading to improved knowledge transfer within the European innovative SME ecosystem;

- Mitigate difficulties in access to finance and new international markets, thereby enhancing the growth and expansion of European innovative SMEs.

Scope: Europe's 25 million small and medium enterprises (SMEs) are the backbone of the EU economy. SMEs can bring innovation to societal challenges, including the security of EU citizens. Innovative SMEs and high-tech start-ups can transform and modernise EU security capabilities.

However, despite the innovation capacity of EU SMEs, these often experience difficulties in finding their way to the public markets. These include red tape in public contracts, access to new customers, access to finance, industrial competition and Intellectual Property (IP) valorisation. These difficulties are exacerbated in markets that show restrictions of different kind, as it is the case of security.

Knowing that SMEs require additional support to reach the security buyers and that the collaboration opportunities offered by the projects of the Pillar II of Horizon Europe can be a catalyst for uptake, this topic aims to offer a collaborative environment for small and medium innovators to tailor their innovations to the specific needs of civil security end-users, taking into account the urge to address the diverse needs of all citizens, regardless of gender, age or ability.

Applicants are invited to submit proposals for technology development along with the following principles:

- Focus on mature technological solutions addressing EU security policy priorities in the areas addressed by the Cluster 3 Work Programme;

- Fostering collaboration between SMEs from different Member States and Associated Countries;

- Involving security end-users in the role of validator and potential first-adopter of the proposed innovations;

- Fostering collaboration schemes between small companies and research and technology organisations and/or big industrial players aimed at fostering innovative technology transfer or creating innovative business models that facilitate access to market and strengthen the innovation capacity of EU SMEs and start-ups in the domain of civil security.

Examples of activities to plan in the proposed projects include, but are not limited to: assimilating market requirements; facilitating access to additional funding; approaching potential public buyers; assess competitive landscape; supporting in innovation management (methodological and process innovation, business model innovation, market innovation); assist in IP management and exploitation; provide guidance for expansion to future markets, etc.

The participation of research and technology organisations should not focus on own technology development but on supporting the small industrial players in accelerating the technology transfer of innovative security solutions for their further development and production.

It is encouraged that one SME takes the coordinator role[172]. If the coordinator is not an SME, this should be duly justified.

The projects should have a maximum estimated duration of 2 years.

Under this topic, projects should address one of the following areas addressed by the Cluster 3 work programme: Fighting Crime and Terrorism (FCT, Option A), Disaster-Resilient Society (DRS, Option B), Resilient Infrastructure (INFRA, Option C), Border Management (BM, Option D).

Some (indicative and non-exhaustive) examples of domains that could be addressed under the FCT area are: mobile forensics; deepfake detection; detection of counterfeiting (fake items, fake currency bills) or falsified/forged documents (passports, ID cards); detection and countering of advanced forms of malware, as well as non-cash payment frauds and other cyber-scams.

Some (indicative and non-exhaustive) examples of domains that could be addressed under the DRS area are: data and satellite/remote sensing information exploitation, positioning and localisation tracking and tracing, monitoring and surveillance for disaster prevention.

Some (indicative and non-exhaustive) examples of domains that could be addressed under the INFRA area are: physical access control, autonomous systems used for infrastructure protection, positioning and localisation tracking and tracing, monitoring and surveillance of environments and activities.

Some (indicative and non-exhaustive) examples of domains that could be addressed under the BM area are: facilitated border checks; secure documents and identity management for border crossings; border surveillance; detection of drugs, explosives, Chemical, Biological, Radiological and Nuclear (CBRN), weapons and/or other dangerous materials in customs environment; detection of stolen, smuggled, illicit or illegal goods (cigarettes, art, cultural goods, wildlife) in a customs environment.

[172] If a MIDCAP is included in the proposal, it could also take the role of coordinator.

Where relevant, proposals are invited to consider legal aspects to support the operationalization, policy integration, and institutional transformation of security solutions. This might include, for instance, the design of legal, policy, and/or standardization pathways to support the operational uptake of security solutions.

This topic contributes to the Strategic Technologies for Europe Platform (STEP[173]) and addresses civil security technologies falling under the sectors of "Digital technologies and deep-tech innovation"[174]. This topic contributes to the objectives stated in the STEP Regulation, e.g., to support the European industry and boost investment in critical technologies in Europe, and, to contribute to reducing or preventing the strategic dependencies of the Union.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2027-01-SSRI-02: Open grounds for future pre-commercial procurement of innovative security technologies**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 1.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 2.00 million. |
| *Type of Action* | Coordination and Support Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility conditions apply:<br>This topic requires the participation, as beneficiaries, of at least 6 end-user organisations as well as at least 3 public procurers. One beneficiary can have the role of end-user and public procurer simultaneously, both counting towards the number of such entities required for the additional eligibility condition. These beneficiaries must be from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security |

173 OJ L, 2024/795, 29.2.2024, ELI: http://data.europa.eu/eli/reg/2024/795/oj
174 https://strategic-technologies.europa.eu/index_en

| | |
|---|---|
| | practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>Open market consultations carried out during this project must take place in at least 3 EU Member States or Associated Countries. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025) [175]. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Establish a consolidated group of potential buyers with shared needs and requirements, committed to carrying out a pre-commercial procurement (PCP) action for future joint procurement of innovative solutions;
- Evidence for Future PCP Action: Provide clear evidence justifying the necessity of a PCP action to complete the maturation cycle of certain technologies and compare different alternatives;
- Increased capacity of EU public procurers to align requirements with industry and future products and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

Scope: End-users and public procurers from several countries are invited to submit proposals for a preparatory action that should build the grounds for a future pre-commercial procurement (PCP) action. Both this preparatory action and the future PCP action are open to proposals oriented to the acquisition of research and development (R&D) services for the development of innovative technologies, systems, tools or techniques under the priorities laid down in this Work Programme.

In preparing the grounds for a possible future PCP action, the outputs of this Coordination and Support Action (CSA) should take into consideration:

[175] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- The policy priorities described in this Work Programme Part for the security areas mentioned above;
- The EU Directive for public procurement and in particular with the provisions related to PCP;
- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe grants, as stated in the General Annex H of the Horizon Europe Work Programme;
- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

During the course of the project, the applicants are expected to deliver clear evidence on a number of aspects in order to justify and de-risk a possible follow-up PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of potential buyers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;
- That the state of the art and the market (including research) has been explored and mapped, and that there are different technical alternatives to address the proposed challenge;
- That a future PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready on due time in order to launch the call for the acquisition of R&D services according to the PCP rules;
- That the technology developments to be conducted in the future PCP can be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data;

- That in developing technology solutions, societal and gender aspects (e.g., perception of security, possible side effects of technological solutions, societal resilience) are taken into account in a comprehensive and thorough manner.

If the applicants intend to submit a proposal for a follow-up PCP in a future Horizon Europe Cluster 3 Work Programme, they should ensure that the above evidence is consolidated in the project deliverables of this CSA before the submission of the PCP proposal.

The project should have a maximum estimated duration of 1 year.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

**HORIZON-CL3-2027-01-SSRI-03: Demand-led innovation in security**

| **Call: Civil Security for Society 2027** | |
|---|---|
| **Specific conditions** | |
| *Expected EU contribution per project* | The Commission estimates that an EU contribution of around EUR 5.83 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative budget* | The total indicative budget for the topic is EUR 5.83 million. |
| *Type of Action* | Pre-commercial Procurement |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>Subject to restrictions for the protection of European communication networks.<br>The following additional eligibility conditions apply:<br>This topic requires the participation[176], as beneficiaries, of at least 3 practitioners and 3 public procurers. These beneficiaries must be from at least 3 different EU Member States or Associated Countries. One organisation can have the role of practitioner and public procurer simultaneously, both counting for the overall number of organisations required for eligibility. Among the public procurers[177], minimum two must be independent legal entities that are public procurers, each established in a different Member State or Associated Country and with |

[176] See General Annexes page 12 on the Consortium Composition as regards Public procurement of innovative solutions.

[177] Under this topic, the participation is required of minimum three procurers as beneficiaries in the buyer's group for the PPI. The third procurer in the buyer's group can be a private procurer or an NGO that provides similar services of public interest as the public procurers.

| | |
|---|---|
| | at least one of them established in a Member State.<br><br>For participants with practitioner status, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.<br><br>If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). |
| *Technology Readiness Level* | Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>The granting authority may, up to 4 years after the end of the action, object to a transfer of ownership or to the exclusive licensing of results, as set out in the specific provision of Annex 5.<br>Beneficiaries may provide financial support to third parties. The support to third parties can only be provided in the form of grants / prizes. The maximum amount to be granted to each third party is EUR 100 000 to provide financial incentives to final end-users that are not part of the consortium (e.g., citizens) to adopt the solutions, including costly hardware components.<br>PCP/PPI procurement costs are eligible.<br>The specific conditions for actions with PCP/PPI procurements in section H of the General Annexes apply to grants funded under this topic.<br><br>Beneficiaries must ensure that the subcontracted work is performed in at least 3 Member States — unless otherwise approved by the granting authority. |

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- A community of EU civil security practitioners with common user/functional needs for innovative technology solutions is identified, supported by an industrial base, in particular SMEs and Startups, to access the public procurement market and scale up their business;

- Procurers facilitate the commercialisation of the innovative solutions developed by their successful suppliers by providing them with first customer references for the validation and first pilot deployment;

- Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes that are accessible and meet the diverse needs of the EU user community, regardless of their gender, age and ability;

- Improved delineation of the EU market (including demand and supply) for innovative civil security systems that can articulate alternative options for uptake in function of different industrialisation needs, commercialisation needs, acquisition needs, deployment needs and additional funding needs (beyond R&I funding).

Scope: As past experience shows that pre-commercial procurement opens up the procurement market for startups and enables the public sector to address societal challenges more effectively, public procurers should make more strategic use of PCP. Applicants are invited to submit proposals for PCP action to acquire Research and Development (R&D) services and innovative civil security technology solutions.

Proposals should demonstrate interest from a broader community of potential buyers, beyond the direct beneficiaries, who share similar needs and are open to jointly adopting the solutions developed, provided they are proven mature and operationally viable. The proposals are expected to include an analysis of the state of the art and market landscape, aligning research activities with identified needs and presenting a range of technical alternatives to address the challenge. Furthermore, to stimulate dialogue with the supply side, public procurers are required to organise proposals that should demonstrate sustainability of the action beyond the life of the project.

The proposals should build on the outcomes of CSA projects funded under previous Horizon Europe work programmes aimed at creating *Stronger grounds for pre-commercial procurement of innovative security technologies*. The proposals should provide clear evidence to justify and de-risk the PCP action, demonstrating that the identified challenge is significant and necessitates a PCP action to mature certain technologies and compare alternatives. It should be shown that a consolidated group of practitioners and procurers with shared needs and requirements is committed to the PCP process, enabling informed decisions on future joint procurement of innovative solutions. Activities covered should include cooperation with policymakers to reinforce the national policy frameworks and mobilise substantial additional national budgets for PCP and innovation procurement in general beyond the scope of the project. The tender process to be followed is described in Annex H.

Proposals should demonstrate commitment to exploiting project results beyond its conclusion, ensuring engagement with stakeholders and implementation of strategies for future uptake. Applicants should also clarify measures to ensure compliance with the principles of the EU Directive on public procurement, particularly those related to PCP. The required open market consultations should be completed in at least three EU Member States. Prior consultations

conducted under previous CSA projects should be used, provided they ensured procurement viability and remain relevant to the current state of the art.

Involvement of procurement decision makers is recommendable to ensure that end solution(s) are adopted by public buyers, increasing the societal impact of the related research activities. Therefore, procurers should declare in the proposal their interest to pursue deployment of solutions resulting from the PCP in case the PCP delivers successful solutions and indicate whether they will:

- Procure successful solution(s) as part of the PCP.
- Launch a separate follow-up procurement after the PCP to buy such type of solutions.
- Adopt successful solutions without the need to procure them (e.g. in case of open-source solutions).
- Foresee financial or regulatory incentives for others to adopt successful solutions (e.g. in case the final end-users of the solutions are not the procurers but for example citizens).

In these four cases, the procurers can implement the project as a fast-track PCP[178]. In the first case, the procurers should foresee the budget in the proposal to purchase at least one solution during the PCP. In the second case, the procurers should include in the proposal a deliverable that prepares the follow-up procurement to purchase such type of solution(s) after the PCP. In the first and third case, the procurers should foresee sufficient time during the project to deploy and validate that the solutions function well after installation. In the fourth case, the procurers can use financial support to third parties to provide financial incentives to final end-users that are not part of the consortium (e.g. citizens) to adopt the solutions, including costly hardware components, with a maximum budget of EUR 100.000.

Applicants should propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalising the tendering documents package for a PCP call for tenders based on the technical input, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.
- Moreover, to ensure the sustainability and uptake of the developed solutions, proposals should outline clear plans for post-PCP activities. As outlined in the general annexes of the Horizon Europe Work Programme 2026-2027, the topic allows public buyers to use the fast-track PCP option (e.g. 2 instead of 3 phases) when they commit to buying or deploying the resulting solutions after the PCP. However, if such a commitment is not yet in place at the proposal stage, the call expects proposers to include a deliverable outlining concrete activities to prepare the ground for follow-up deployment or procurement after the PCP.

178 See General Annex H of the Horizon Europe Work Programme.

- Launching the call for tenders for research and development services. The call for tenders should envisage a competitive development composed of different phases that would lead to at least 2 prototypes from 2 different providers to be validated in real operational environment at the end of the PCP cycle;

- Conducting the competitive development of the prototypes following the PCP principles including a design phase, an integration and technical verification phase and a validation in real operational environment phase. In evaluating the proposals and the results of the PCP phases, the applicants should consider technical merit, feasibility and commercial potential of proposed research efforts.

- Consolidating the results of the evaluation of the developed prototypes, extracting conclusions and recommendations from the validation process, and defining a strategy for a potential uptake of solutions inspired in the PCP outcomes, including a complete technical specification of the envisaged solutions and standardisation needs and/or proposals. This strategy should consider joint-cross border procurement schemes and exploit synergies with other EU and national non-research funds.

Applicants are expected to maximise the visibility of the project outcomes to the wide community of potential EU public buyers. Liaison with other civil security communities beyond those addressed by the project is encouraged in order to assess the possible reuse and extensibility of the identified solutions to different domains.

Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Strengthened Security Research and Innovation Destination.

## Other actions not subject to calls for proposals

### 1. External expertise for reviews of projects

This action will support the use of appointed independent experts for the monitoring of actions (grant agreement, grant decision, public procurement actions, financial instruments) funded under Horizon Europe and previous Framework Programmes for Research and Innovation, and where appropriate include ethics checks, as well as compliance checks regarding the Gender Equality Plan eligibility criterion[179].

Form of Funding: Other budget implementation instruments

Type of Action: Expert contract action

Indicative timetable: 1st quarter 2026 and 1st quarter of 2027

Indicative budget: EUR 0.80 million from the 2026 budget and EUR 0.80 million from the 2027 budget

### 2. Workshops, conferences, experts, communication activities, studies and innovation uptake promotion

- Organisation of the annual Security Research Event.
- Support to workshops, expert groups, communications activities, or studies. Workshops are planned to be organised on various topics to involve end-users (e.g. the Community for European Research and Innovation for Security); preparation of information and communication materials, etc.
- Organisation of cybersecurity conferences and support to other cybersecurity events; socio-economic studies, impact analysis studies and studies to support the monitoring, evaluation and strategy definition for cybersecurity and digital privacy policy.
- Support to promotion of innovation uptake, including through supporting developing certification testing methodologies for innovative technologies.
- Needs analysis and options for enabling the sharing of security research projects outputs (tools).

Form of Funding: Procurement

Type of Action: Public procurement

Indicative timetable: 1st quarter 2026 and 1st quarter of 2027

[179] *The Commission intends to transfer to the ECCC an indicative amount of 0.085 M EUR from 2026 and 0.12 M EUR from 2027 related to the implementation of the delegated grant agreements. See indirectly managed action delegated to the ECCC.*

Indicative budget: EUR 2.13 million from the 2026 budget and EUR 1.52 million from the 2027 budget

### 3. Indirectly Managed Action by the ECCC (2026)

The Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878. In particular, the contribution agreement will entrust the ECCC with the implementation of a call for proposals according to the specifications in the Appendix set out below. Further to the contribution agreement, the ECCC will launch a call for proposals in accordance with the specifications in the Appendix set out below. These include topics where participation will be limited in accordance with Article 22(5) of the Horizon Europe Regulation to legal entities established in Member States and Horizon Europe Associated Countries (eligible countries). In addition, for such topics, in order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, will not be eligible to participate.

Legal entities:

European Cybersecurity Competence Centre (ECCC), Polytechnic University of Bucharest, Strada Splaiul Independentei Nr.313, Sector 6, Bucharest 060042, Romania

Form of Funding: Indirectly managed actions

Type of Action: Indirectly managed action

Indicative budget: EUR 56.20 million from the 2026 budget

**APPENDIX – Indirectly managed action by the ECCC 2026**

**Specifications of the 'Cybersecurity' call to be launched by ECCC**

**Call - Cybersecurity**

***HORIZON-CL3-2026-02-CS-ECCC***

**Conditions of the call**[180]

Proposals are invited against the following topic(s):

| Topics | Type of | Budgets | Expected | Indicative |
|---|---|---|---|---|

[180] The Executive Director-of the ECCC may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Executive Director of the ECCC may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2026.

| | Action | (EUR million) | EU contribution per project (EUR million)[181] | number of projects expected to be funded |
|---|---|---|---|---|
| | | 2026 | | |
| Opening: 3 March 2026<br>Deadline(s): 15 September 2026 | | | | |
| HORIZON-CL3-2026-02-CS-ECCC-01:Approaches and tools for security in software and hardware development and assessment | RIA | 20 | 3-4 | 4-5 |
| HORIZON-CL3-2026-02-CS-ECCC-02:Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI) | IA | 21.2 | 3-4 | 4-5 |
| HORIZON-CL3-2026-02-CS-ECCC-03:Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations | RIA | 15 | 2-3 | 3-4 |
| Overall indicative budget | | 56.2 | | |

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

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per Project:* | The Commission estimates that an EU contribution of between EUR 3 and 4 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is 20 million. |
| *Type of Action:* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this |

[181] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | |
|---|---|
| | topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Procedure* | The procedure is described in General Annex F. The following exceptions apply:<br>To ensure a balanced portfolio covering a broad range of research areas, grants will be awarded to applications not only in order of ranking but at least also to the two highest ranked proposal addressing expected outcome a) and the highest ranked proposal addressing expected outcome b), provided that the applications attain all thresholds. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[182]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute to one or more of the following:

- Enhanced security frameworks for both hardware and software supply chains, building on root-of-trust architectures and secure lifecycle management;
- Secure and trusted chip architectures for next-generation computing and networking systems;

[182] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Integrated security-by-design approaches in software development, aimed to be aligned with relevant regulatory requirements;
- Security testing methodologies, including formal verification approaches and AI-driven security testing methodologies;
- Standardised methodologies for hardware security assessment, also contributing to cybersecurity certification.

**Scope:**

The increasing complexity and globalisation of software and hardware supply chains introduce new vulnerabilities that cyber adversaries can exploit. Ensuring the security of both software and hardware components across the lifecycle of digital systems is paramount. This topic aims to develop innovative tools, methods, and processes to secure the entire ecosystem of software and hardware development.

Proposals **should explicitly select one main area of focus but can also address both:**

a. Secured hardware systems over trusted Chips

The security of modern computing infrastructures relies heavily on the robustness of hardware components. This subtopic aims to develop robust security solutions for trusted hardware platforms, focusing on secured microprocessors, secure boot mechanisms, and cryptographic acceleration. Proposals are also expected to address the risks of hardware-based vulnerabilities and backdoors, ensuring the security of devices from edge to cloud, also taking into account emerging threats, including quantum where relevant. Synergies with existing EU initiatives on trusted hardware (e.g., CHIPS JU, EuroHPC) are encouraged. The topic is expected to:

- Develop new architectures for tamper-resistant chips and processors. Exploring novel designs for secure microprocessors, leveraging hardware-level security enhancements, and integrating cryptographic co-processors that may also support post-quantum cryptography (PQC), for enhanced protection against tampering and side-channel attacks.
- Enhance supply chain transparency for chip production and integration. Exploring innovative ways to improve traceability and accountability in chip manufacturing processes, including methods such as post-quantum secure hardware roots of trust, blockchain for tracking components, or certification mechanisms.
- Establish security-by-design methodologies for hardware security assessment. Advancing methodologies for systematic security testing of hardware components, including automated vulnerability analysis, verification frameworks, and integration of security assessment into chip design and lifecycle management.

- Develop methods and tools for an effective and efficient non-destructive authentication and physical analysis of integrated circuits and multi-chips modules (chiplets).

- Develop technical means for ensuring hardware supply chain security, and secure PQC implementations: hardware trojan and backdoor detection, hardware watermarking, relevant reverse engineering techniques, countermeasures also against new classes of hardware physical attacks. Develop self-healing firmware able to recover from cyber-attacks. Develop firmware able to leverage advanced anomaly detection, AI-driven threat mitigation and secure rollback mechanisms to automatically identify cyber-attacks, isolate compromised components restore the system to a trusted state while maintaining operational continuity.

b. Software Supply Chain security

The integrity of software supply chains is critical to mitigating cybersecurity threats such as supply chain attacks, dependency vulnerabilities, and compromised software components. This subtopic focuses on mitigating security risks in software supply chains, including secure code provenance, automated vulnerability detection, and secure software development lifecycle (SDLC) methodologies and tools, including those related to PQC security. Proposals should integrate formal verification approaches or AI-assisted security testing, leveraging upcoming European and International standards for supply chain security. The topic is expected to:

- Develop innovative tools for real-time software vulnerability detection and automatic patching. Advancing the state of automated detection techniques, incorporating dynamic analysis, AI-driven pattern recognition, predictive analytics to proactively identify security weaknesses before exploitation and self-healing mechanisms.

- Enhance secure software frameworks, including protection against the quantum threat. Exploring new methodologies for integrating security-by-design principles across development workflows, incorporating approaches such as automated security policy enforcement, modular security components, and improved dependency management.

- Improve resilience against supply chain cyber threats. Investigating novel mitigation strategies, including provenance tracking for software components and their analysis, secure update distribution mechanisms including protection from emerging quantum threats where relevant, enhanced anomaly detection, and multi-layer defence approaches to ensure integrity and trustworthiness.

**HORIZON-CL3-2026-02-CS-ECCC-02: Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per* | The Commission estimates that an EU contribution of between EUR 3 and 4 million would allow these outcomes to be addressed |

| | |
|---|---|
| *Project:* | appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 21.2 million. |
| *Type of Action:* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[183]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute to one or more of the following:

- Robust AI models and systems capable of resisting different classes of adversarial manipulation;
- Innovative defence mechanisms for AI models and systems against new attack families;

[183] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Methodologies for detecting and mitigating attacks, such as data poisoning, backdoor exploitation and misclassification;
- AI systems leveraging privacy-enhancing technologies that maintain data confidentiality and regulatory compliance, enabling trusted in-house AI deployments (e.g., for governments and enterprises).

**Scope:**

The increasing reliance on AI in cybersecurity, critical infrastructure, and decision-making processes raises concerns about the security and robustness of AI systems. As AI systems become more prevalent, they are increasingly targeted by adversarial attacks that manipulate inputs, compromise training data, or introduce hidden vulnerabilities. This topic aims to strengthen the resilience of AI systems and algorithms against various threats and attacks, such as enhancing their resilience against adversarial attacks, backdoor injections, and data poisoning. Proposals should develop real-time anomaly detection, mitigation techniques to defend against adversarial attacks and robust federated learning techniques, in synergies with leading efforts on AI transparency, and in compliance with the AI Act. The topic is expected to:

- Develop robust AI models resistant to adversarial attacks. Exploring techniques to harden AI models and systems against adversarial perturbations, such as adversarial training, robust optimisation, and defence mechanisms that enhance the trustworthiness of AI.
- Improve detection of manipulated or poisoned training data. Advancing methodologies to identify and mitigate compromised datasets, leveraging techniques such as anomaly detection, provenance tracking, and automated data validation mechanisms.
- Address the concept of Private AI by developing mechanisms that enable AI models to be trained, deployed and operated in privacy-preserving environments, particularly for sensitive use cases, as for example for government and enterprise settings. This includes ensuring AI computations and data remain within trusted execution boundaries (e.g. on-premise or regulated cloud environments), and leveraging existing and emerging privacy-enhancing techniques such as federated learning, secure aggregation, computing on encrypted data, quantum-safe homomorphic encryption and secure inference in deep learning to safeguard the protection of personal and other sensitive data throughout the AI lifecycle.

**HORIZON-CL3-2026-02-CS-ECCC-03: Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per* | The Commission estimates that an EU contribution of between EUR 2 and 3 million would allow these outcomes to be addressed |

| | |
|---|---|
| *Project:* | appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 15 million. |
| *Type of Action:* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[184]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute to one or more of the following:

- Quantum-resistant cryptographic primitives, also other than lattice-based approaches if relevant, that enhance the security and privacy of digital wallets, both for natural persons and wallets, as well as the design and implementation of post-quantum solutions for entity authentication and authenticated key establishment over insecure networks;

[184] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Formal verification tools, improved High-Assurance Cryptographic Software (HACS) approaches and their integration in software workflows, to provide strong security guarantees in post-quantum migration, and enable streamlined evidence-based evaluation of secure systems that use cryptography.

**Scope:**

The development of new digital signatures and advanced cryptographic schemes, tailored specifically to the use cases and requirements in the context of wallets/eIDs, for privacy and business applications is highly relevant nowadays. Moreover, these devices need secure connections over insecure networks requiring protocols for entity authentication, authenticated key establishment, as well as Password Authenticated Key Exchange (PAKE) schemes for ensuring user authentication via passwords in different use cases and for data recovery protocols of Wallet data.

Another key area is the development of High-Assurance Cryptographic Software (HACS), including automated evaluation methods.

Considering the above, proposals should address one of the following technology areas:

- Design and implementation of PQC advanced schemes and protocols for enhanced security and privacy, also including schemes other than lattice-based approaches if relevant. Proposals should also include recommendations that balance security, performance, and usability in practical applications and be based on open-source reusable software libraries.

- Development of a unified specification language to formalise and document conditions on cryptographic safety and security in software implementations; development and improvement of tools and methodologies that can be used to evaluate both the implementation and the usage of cryptography in software applications and provide formal machine-checked guarantees of correctness and security. Proposals should also consider improving existing HACS tools and their integration in such software implementations.

**4. Indirectly Managed Action by the ECCC (2027)**

The Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878. In particular, the contribution agreement will entrust the ECCC with the implementation of a call for proposals according to the specifications in the Appendix set out below. Further to the contribution agreement, the ECCC will launch a call for proposals in accordance with the specifications in the Appendix set out below. These include topics where participation will be limited in accordance with Article 22(5) of the Horizon Europe Regulation to legal entities established in Member States and Horizon Europe Associated Countries (eligible countries). In addition, for such topics, in order to guarantee

the protection of the strategic interests of the Union and its Member States, entities established in an eligible country, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, will not be eligible to participate.

Legal entities:

European Cybersecurity Competence Centre (ECCC), Polytechnic University of Bucharest, Strada Splaiul Independentei Nr.313, Sector 6, Bucharest 060042, Romania

Form of Funding: Indirectly managed actions

Type of Action: Indirectly managed action

Indicative budget: EUR 71.80 million from the 2027 budget

**APPENDIX – Indirectly managed action by the ECCC 2027**

**Specifications of the 'Cybersecurity' call to be launched by ECCC**

**Call - Cybersecurity**

***HORIZON-CL3-2027-02-CS-ECCC***

**Conditions of the call**[185]

Proposals are invited against the following topic(s):

| Topics | Type of Action | Budgets (EUR million) | Expected EU contribution per project (EUR million)[186] | Indicative number of projects expected to be funded |
|---|---|---|---|---|
| | | 2027 | | |
| Opening: 2 March 2027<br>Deadline(s): 15 September 2027 | | | | |
| HORIZON-CL3-2027-02-CS-ECCC-01:Artificial Intelligence for Cybersecurity applications | RIA | 24.8 | 4-5 | 5-6 |

[185] The Executive Director-of the ECCC may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Executive Director of the ECCC may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2027.

[186] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

| | | | | |
|---|---|---|---|---|
| HORIZON-CL3-2027-02-CS-ECCC-02: Secure Computing Continuum (IoT, Edge, Cloud, Data spaces) | IA | 24 | 4-5 | 5-6 |
| HORIZON-CL3-2027-02-CS-ECCC-03: Secure PQC implementations, Cryptanalysis and Post-quantum Digital Trust | RIA | 19 | 3-4 | 4-5 |
| HORIZON-CL3-2027-02-CS-ECCC-04: New primitives for functionalities of future hybrid quantum-classical and quantum networks | RIA | 4 | 4 | 1-2 |
| Overall indicative budget | | 71.8 | | |

**HORIZON-CL3-2027-02-CS-ECCC-01: Artificial Intelligence for Cybersecurity applications**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per Project:* | The Commission estimates that an EU contribution of between EUR 4 and 5 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 24.8 million. |
| *Type of Action:* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for |

| | |
|---|---|
| | Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[187]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute to one or more of the following:

- AI-driven solutions for real-time cyber threat detection;
- Advanced adaptive AI systems that evolve with dynamic cybersecurity challenges;
- Contribute to drastically reduce reaction time for the recovery of systems.

**Scope:**

Artificial Intelligence is increasingly utilised in cybersecurity for threat detection, incident response, and adaptive defence mechanisms. However, AI-driven systems themselves are susceptible to adversarial manipulation and bias. This topic aims to advance AI-based cybersecurity applications while ensuring that AI-driven solutions remain resilient, transparent, and compliant with regulatory frameworks such as the AI Act. In this context, the topic explores the role of all types of AI, including generative AI, in cybersecurity applications, including automated threat detection, adaptive cyber defence, and AI-driven cyber threat intelligence. Proposals should develop solutions for trustworthy AI in cybersecurity contexts including addressing adversarial AI risks, in compliance with the provisions of the AI Act. The topic is expected to:

- Develop AI-driven solutions and tools for real-time cyber threat detection. Investigating novel machine learning techniques to detect anomalies, malicious activity, and AI-powered cyber threats in real time, improving situational awareness and response times.
- Develop adaptive AI systems capable of evolving with dynamic cybersecurity challenges. Exploring AI techniques that continuously learn from new cyber threats, adapting to emerging attack patterns, while maintaining robustness and explainability.
- Support the future enhancements of Security Operation Centres/Cyber Hubs. Developing AI-enhanced SOC frameworks that integrate predictive analytics, automation, and threat intelligence to strengthen proactive defence measures.

[187] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

**HORIZON-CL3-2027-02-CS-ECCC-02: Secure Computing Continuum (IoT, Edge, Cloud, Data spaces)**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per Project:* | The Commission estimates that an EU contribution of between EUR 3 and 4 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 24 million. |
| *Type of Action:* | Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[188]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute to one or more of the following:

[188] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Enhanced resilience against distributed cyber threats and adversarial attacks targeting interconnected systems, while preserving data privacy in highly dynamic and heterogeneous environments;

- Security solutions tailored to distributed computing systems including for example IoT and edge computing environments, integrating privacy-preserving mechanisms;

- Improved interoperability of security measures and cross-layer security, including the compatibility of privacy-enhancing technologies across different layers of the computing continuum and data spaces, and across providers in the multi-provider edge cloud continuum.

**Scope:**

This topic aims to advance security across the entire computing continuum, spanning IoT devices, edge computing, cloud infrastructures, AI computing environments, and data spaces. Proposals should address critical challenges such as ensuring data integrity in highly distributed and dynamic environments, implementing robust zero-trust architectures to secure interconnected and heterogeneous systems, and enabling comprehensive protection for sensitive data and processes. Privacy should be considered a core element of these approaches, ensuring that data confidentiality is preserved throughout its lifecycle, in compliance with relevant data protection frameworks, such as GDPR. Solutions are expected to deliver tangible and measurable security improvements across all layers of the continuum, prioritizing scalability, interoperability, trustworthiness, security and resilience against emerging threats.

Proposals are expected to address one or more of the following:

- Develop advanced security solutions for edge to cloud. For example, investigating lightweight cryptographic techniques, including in combination with or based on post-quantum cryptography, incorporated in zero-trust architectures, and decentralized security models to ensure end-to-end protection from edge to cloud, while maintaining privacy during data transmission and processing.

- Enhance interoperability of security measures across different computing layers. Exploring security protocols, identity and access management solutions, and cross-domain authentication mechanisms to seamlessly integrate security controls across diverse computing ecosystems, including privacy-preserving protocols that enable the secure and compliant data exchange.

- Develop portable, deployable PQC acceleration solutions through SW/HW secure co-design to secure user data and computing tasks across heterogeneous platforms and applications in all layers of the continuum.

- Improve resilience against distributed cyber threats. Exploring anomaly detection, including AI-driven anomaly detection, intrusion prevention techniques, and automated response mechanisms to counter emerging threats targeting interconnected

infrastructures and data spaces, while upholding privacy through techniques such as federated analysis, secure multi-party computation, Fully Homomorphic Encryption or other.

Proposals are encouraged to develop synergies with activities and projects in HE Cluster 4.

**HORIZON-CL3-2027-02-CS-ECCC-03: Secure PQC implementations, Cryptanalysis and Post-quantum Digital Trust**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per Project:* | The Commission estimates that an EU contribution of between EUR 3 and 4 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 19 million. |
| *Type of Action:* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The procedure is described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[189]. |
| *Security Sensitive* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and |

[189] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

| | |
|---|---|
| *Topics:* | SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected Outcome:**

Proposals are expected to contribute one or more of the following:

- Practical robust implementations of PQC schemes that can withstand implementation attacks including side-channel attacks, fault attacks and combined attacks, and design of automated tools for evaluating the security of PQC implementations. Comprehensive guidelines for implementing countermeasures against a wide range of attacks;
- Advances in understanding the quantum hardness of mathematical problem classes; new quantum algorithms and improvements in quantum programming and implementation; security validation methods; design of post-quantum schemes with improved security against quantum and AI-based attacks;
- Post-quantum schemes and protocols to support privacy-friendly applications and services, including the secure and private use of electronic identities. Design of new digital signatures, key encapsulation mechanisms, and other schemes or use of existing ones to build new verification protocols.

**Scope:**

Securing PQC algorithm implementations is vital to protect against implementation attacks, such as side channel attacks, fault attacks and combinations of these, which may be amplified by deep learning. Current countermeasures incur significant overhead, and new approaches are needed to balance security and performance. Formal verification tools and methodologies can help achieve this goal and provide machine-readable evidence. Furthermore, to boost confidence in PQC systems, their security should be assessed, including the potential impact of new quantum algorithms or new optimizations of existing ones, also combined with AI.

Another key research area is digital trust in the post-quantum era, which requires transforming various areas, such as secure identities, data protection, access to essential services, and applications such as backup recovery, browser extensions and others into trusted and reliable solutions, via new post-quantum schemes and advanced building blocks for privacy-enhancing protocols.

Proposals should address one of the following technology areas:

- Development of solutions to prevent implementation attacks, balancing security, performance and cost; research in new attacks, including AI-powered ones, and/or combination of attacks, to inform secure design; creation of testing frameworks for automated security evaluations; improvement of formal verification methodologies.
- Quantum hardness analysis, via the study of the impact of new quantum algorithms or improvement of existing quantum algorithm implementations as well as the impact of

AI-supported quantum attacks; analysis of cryptanalysis results; design of new post-quantum schemes using the information of the advances achieved/ fine-tuning of parameters sets.

- Design of quantum-resistant schemes and protocols supporting the field of privacy-friendly applications and services, including electronic identities, verification protocols and pseudonymous access options, protocols for attestation and anonymous attestation, for real world scenarios, via the design of new digital signature schemes and key encapsulation mechanisms, design of advanced cryptographic schemes, and usage of existing schemes in new protocols, for post-quantum digital identity and digital trust systems.

**HORIZON-CL3-2027-02-CS-ECCC-04: New primitives and protocols for functionalities of future hybrid classical-hybrid and quantum networks**

| *Specific Conditions* | |
|---|---|
| *Expected EU Contribution per Project:* | The Commission estimates that an EU contribution of 4 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts. |
| *Indicative Budget:* | The total indicative budget for the topic is EUR 4 million. |
| *Type of Action:* | Research and Innovation Actions |
| *Eligibility conditions* | The conditions are described in General Annex B. The following exceptions apply:<br>In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action. |
| *Legal and financial set-up of the Grant Agreements* | The rules are described in General Annex G. The following exceptions apply:<br>Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the |

| | |
|---|---|
| | Research and Training Programme of the European Atomic Energy Community (2021-2025)[190]. |
| *Security Sensitive Topics:* | Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes. |

**Expected outcome:**

Proposals are expected to contribute to one or more of the following:

- New primitives beyond Quantum Key Distribution (QKD) for future hybrid classical-quantum and quantum networks either as quantum equivalents of classical primitives or as new primitives for new practical applications, also in the relativistic setting when relevant, or as new primitives and protocols with modular, realistic integration of solutions from different cryptographic approaches, with focus on beyond-QKD applications and with gradual release on trust in hardware;
- Analysis of the applicability and strength of the results compared to their best classical-only counterpart, critical analysis of the formal assumptions and of performance, security proofs;
- Investigation of fundamental aspects of quantum information processing tasks, their eventual limits; and/or the connection between quantum computing and cryptography for insights for stronger cryptographic foundations;
- Roadmap for quantum cryptography and networks functionalities.

**Scope:**

The action supports research on new primitives and protocols beyond QKD for security and trust-based applications, by combining different cryptographic approaches and by exploiting insights from quantum information science, to demonstrate compelling quases of quantum cryptographic advantage and obtain foundational results on the unique features of quantum protocols. The goal is to build on the basis of insights from the field of real-world, applied cryptography and the vision from the quantum domain on future entanglement-based networks, the foundations of a new cryptography, that will support mid-term hybrid classical-quantum and further in the future almost fully quantum networks. The design of such new foundations may need entirely new paradigms whose design requires different expertise.

The proposal should target some of the following areas and lead to a roadmap:

[190] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link:https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Development of quantum primitives which have classical equivalent, of new quantum primitives not possible classically (or without trusted hardware), and of alternative solutions improving quantum cryptography protocols using classical cryptography solutions (in particular PQC), by flexibly incorporating various cryptographic components, with some beneficial aspects such as performance improvements (run time, energy usage, less requirements on HW etc.)

- Analysis of the applicability and strength of the results compared to their best classical-only counterpart, critical analysis of the formal assumptions, rigorous security proofs, case-by-case analysis of composable security and of performance.Connection between quantum information processing tasks and holography, and transfer to the cryptographic context, such as, among others, non-local quantum computation for position-verification schemes and spoofing schemes as means of establishing trust, via foundational insights on entanglement and quantum correlations; connection between quantum computing and cryptography providing stronger cryptographic foundations.

- Development of a quantum cryptography roadmap, which identifies challenges for the technical realisation and scaling of applications and presenting the implications for the best hardware and architecture settings for both near-term and long-term applications of quantum networks.

Proposals should include, in a balanced manner, quantum scientists and researchers from PQC with experience on real-world, applied cryptography and with interest in quantum protocols and new paradigms for future networks.

## Budget[191] [192]

| | Budget line(s) | 2026 Budget (EUR million) | 2027 Budget (EUR million) |
|---|---|---|---|
| **Calls** | | | |
| HORIZON-CL3-2026-01 | | 131.00 | |
| | *from 01.020230* | *131.00* | |
| HORIZON-CL3-2027-01 | | | 129.50 |
| | *from 01.020230* | | *129.50* |
| **Other actions** | | | |
| Expert contract action | | 0.80 | 0.80 |
| | *from 01.020230* | *0.80* | *0.80* |
| Public procurement | | 2.13 | 1.52 |
| | *from 01.020230* | *2.13* | *1.52* |
| Indirectly managed action | | 56.20 | 71.80 |
| | *from 01.020230* | *56.20* | *71.80* |
| **Estimated total budget** | | 190.13 | 203.62 |



191 The budget figures given in this table are rounded to two decimal places.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2026 and 2027.

192 The contribution from Cluster 3 for year 2026 is EUR 9.51 million for the Missions work programme part and EUR 1.75 million for the New European Bauhaus Facility work programme part.
The contribution from Cluster 3 for year 2027 is EUR 11.51 million for the Missions work programme part and EUR 2.05 million for the New European Bauhaus Facility work programme part.