EN

Horizon Europe

Work Programme 2023-2024

6. Civil Security for Society

(European Commission Decision C(2022)7550 of 6 December 2022)

Table of contents

Introduction

Supporting EU policy priorities

This Cluster 3 Work Programme will support the implementation of EU policy priorities on security, including cybersecurity, and disaster risk reduction and resilience. In addition, it will build on lessons learnt from the COVID-19 pandemic to strengthen prevention, mitigation, preparedness and capacity building for crises (including health crises) and to improve cross-sectoral aspects of such crises. In this respect, this Work Programme will therefore also ensure synergies and coordination of actions with other parts of Pillar 2.

The Work Programme will support the European Commission policy priority '*Promoting the European way of life*', as well as '*European Green Deal*' and '*Europe fit for the digital age*'. It will in particular support the implementation of the **Security Union Strategy**[1], the **Counter-Terrorism Agenda**[2], the **EU Strategy to tackle Organised Crime**, the **EU Strategy on Combatting Trafficking in Human Beings**, the **EU strategy for a more effective fight against child sexual abuse,** the **EU Action Plan on firearms trafficking**, the border management and security dimensions of the **Pact on Migration and Asylum**[3], **EU Disaster Risk Reduction policies,** the **EU Climate Adaptation Strategy**[4], the **EU Maritime Security Strategy** and the **EU Cybersecurity Strategy**[5].

Within the framework of the Horizon Europe Strategic Plan 2021-2024, the Cluster 3 expected impacts will contribute in particular to the impact areas "*A resilient EU prepared for emerging threats*" and "*A secure, open and democratic EU society*" of Key Strategic Orientation D "*Creating a more resilient, inclusive and democratic European society*" and to the impact area "*Secure and cybersecure digital technology*" of Key Strategic Orientation A "*Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains*".

Meeting capability requirements

Projects will develop new knowledge, technologies and/or other solutions to the identified requirements. Projects will involve practitioner end-users (usually relevant national authorities) alongside researchers and industry. Such involvement has shown their added value in ensuring that the results of R&I are targeted to practitioners' needs[6]. Relevant requirements are specified for the different topics.

Projects need to show their contribution to a wider needs-driven capability development cycle that triggers research, steers its implementation and capitalises on its outcomes. This means

1 COM(2020) 605 final.
2 COM(2020) 795 final.
3 COM(2020) 609 final.
4 COM(2021) 82 final.
5 JOIN(2020) 18 final.
6 Such as capability gaps identified by IFAFRI – International Forum to Advance First Responder Innovation www.internationalresponderforum.org

that projects need to show, on the one hand, an understanding of the capability requirement that has led to the R&I need, and, on the other hand, a strategy for ensuring the uptake of the outcomes including opportunities for using relevant EU funds for funding deployment.

Ensuring ethical outcomes that are supported by society

In the field of security research, it is particularly important that projects take into account human factors and the societal context, and ensure the respect of fundamental rights, including privacy and protection of personal data. Citizens and communities 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 better integrated into security research. Again, relevant requirements are specified for the different topics. Social innovations should also be considered, notably because new tools, ideas and methods lead to active citizen engagement and as drivers of social change and social ownership.

The six Destinations

This Work Programme comprises the following six Destinations that (i) build on the structure of the Horizon 2020 work programmes for security research and (ii) respond to the following expected impacts of Cluster 3 in the Horizon Europe Strategic Plan 2021-2024:

1. Destination – Better protect the EU and its citizens against crime and terrorism

Expected Impact: "*Crime and terrorism are more effectively tackled, while respecting fundamental rights, […] thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for police authorities […] including measures against cybercrime."*

2. Destination – Effective management of EU external borders

Expected Impact: *"Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."*

3. Destination – Resilient infrastructure

Expected Impact: *"[…] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructure operators […]"*

4. Destination – Increased Cybersecurity

Expected 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.*"

5. Destination - A Disaster-Resilient Society for Europe

Expected Impact: *"Losses from natural, accidental and human-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness, and resilience and improved disaster risk management in a systemic way."*

6. Destination –Strengthened Security Research and Innovation

In addition, a number of cross-cutting R&I actions will support all of the above expected impacts:

- *generate knowledge and value in cross-cutting matters in order to avoid sector-specific bias and to break silos that impede the proliferation of common security solutions;*
- *support innovation uptake and go-to-market strategies with the aim of paving the way towards an increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research, thus contributing to reinforce the competitiveness of EU security industry and safeguard the security of supply of EU products in key security areas.*

Under each Destination, before the texts of the topics themselves, there is an important introductory part that explains the relevant policy objectives, that specifies any elements to be taken into account for all the topics of the Destination, including international cooperation- and that identifies specific expected impacts. Proposals should set out a credible pathway to contributing to those specific expected impacts.

International cooperation

In line with the EU's Global Approach to Research and Innovation, and as for the Work Programme 2021-2022, the Work Programme 2023-2024 will remain almost completely open to the participation of non-associated Third countries to all topics. In support of the Global Gateway Strategy, projects involving international partners should lead to increased scientific knowledge and transfer of technology among partner countries allowing to address global challenges across the world and create sustainable growth and jobs. Cooperation should take place in a value-based way, creating linkages, not dependencies.

Security research under Cluster 3 requires a specific approach towards international cooperation to achieve the right balance between the need to exchange with key international partners (including with relevant international organisations), while at the same time ensuring

the protection of the EU security interest and respecting the need for open strategic autonomy in critical sectors.

Within the Destination 'A Disaster-Resilient Society for Europe', there is an established culture of comprehensive collaboration with third countries under the different security research programmes, taking due account of the trans-national dimension of different natural and human-made hazards and their drivers (such as climate change). Therefore, in this Destination, international cooperation will be strongly encouraged given the value of cooperating internationally in particular in developing technologies for first responders. Cooperation can include sharing knowledge, experiences, expertise and mutual learning on disaster-risk management.

As for the Destinations relating to protecting against crime and terrorism, to border management, to infrastructure resilience and to cybersecurity, international cooperation is explicitly encouraged only where appropriate and specifically supporting ongoing collaborative activities. Due to the sensitive nature of most projects in those areas and the obvious interest of the EU to ensure confidentiality of projects results, as well as maintaining the ability to maintain open strategic autonomy in critical domains of security, such explicit cooperation will need to be assessed at the level of topics and limited to selected international partners only. In line with the overall strategic approach to Research and Innovation policy, cooperation would need to be based on reciprocity and contribute to wider strategic goals of the EU.

Applicants are reminded that legal entities established in China are not eligible to participate in Innovation Actions in any capacity. Please refer to the Annex B of the General Annexes of this Work Programme for further details.

Synergies with other funding instruments

In this cluster, the main synergies to be sought are sequential with Horizon Europe funding R&I activities being followed by final development and market uptake and deployment of relevant research results for which funding will in particular be sought from:

- Integrated Border Management Fund (IBMF), consisting of the Border Management and Visa Instrument (BMVI) and the Customs Control Equipment Instrument – for border capabilities.
- Internal Security Fund (ISF) – for law enforcement capabilities.
- Digital Europe Programme[7] – for cybersecurity capabilities and law enforcement digital capabilities. The programme will speed up the take-up of R&I projects in the area of Artificial Intelligence, High Performance computer and cyber security. The programme will also offer infrastructure to the research community.

[7] REGULATION (EU) 2021/694 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

- Cohesion policy, in particular through the European Regional Development Fund (ERDF[8]) – notably managing disaster risks, adapting to climate change, protecting public spaces and utilities (including for energy, transport) and cybersecurity, as well as interregional cooperation on these issues.

Synergies with other funds should also be articulated in a way that accelerates market uptake of successful outcomes of R&I actions. To that end, the complementarity of funding instruments should be considered under a wider capability development cycle.

While actions under Horizon Europe should have an exclusive focus on civilian applications, synergies should be sought with the activities funded under the European Defence Fund or its precursor programmes (Preparatory Action on Defence Research and European Defence Industry Development Programme) while avoiding unnecessary duplication.

In addition, synergies can be sought with the Union Civil Protection Mechanism, including via opportunities such as the Union Civil Protection Knowledge Network, Prevention & Preparedness projects, developing additional reserve capacities under rescEU for major and simultaneous disasters, and by co-financing the deployment of Member States' national response capacities.

[8] "Synergies between Horizon Europe and ERDF programmes (Draft Commission Notice)" https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/synergies-guidance-out-2022-07-06_en

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

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: *"Crime and terrorism are more effectively tackled, while respecting fundamental rights, […] thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for police authorities […] including measures against cybercrime."*

More specifically, 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, domestic and sexual violence, or juvenile offenders;
- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);
- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;
- More secure cyberspace for citizens, especially children, through a robust prevention, detection, and protection from cybercriminal activities.

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

- the involvement of the Police Authorities in their core,
- 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.),
- 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,
- a robust plan on how they will build on the relevant predecessor projects,

- the (active) involvement of citizens, voluntary organisations and communities,
- education and training aspects, especially for Police Authorities and other relevant practitioners, 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,
- 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) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-FCT-01	36.00		23 Nov 2023
HORIZON-CL3-2024-FCT-01		33.70	20 Nov 2024
Overall indicative budget	36.00	33.70	

Call - Fighting Crime and Terrorism 2023

HORIZON-CL3-2023-FCT-01

Conditions for the Call

Indicative budget(s)[9]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[10]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-FCT-01-01	IA	7.00	Around 7.00	1
HORIZON-CL3-2023-FCT-01-02	IA	9.00	Around 4.50	2
HORIZON-CL3-2023-FCT-01-03	RIA	4.00	Around 4.00	1
HORIZON-CL3-2023-FCT-01-04	RIA	4.00	Around 4.00	1
HORIZON-CL3-2023-FCT-01-05	RIA	4.00	Around 4.00	1
HORIZON-CL3-2023-FCT-01-06	RIA	8.00	Around 4.00	2
Overall indicative budget		36.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General

[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 years 2023 and 2024.

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

	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.

FCT01 - Modern information analysis for fighting crime and terrorism

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-01: Processing of large, complex and unstructured datasets resulting from criminal investigations, while reconciling big data analysis and data protection

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 7.00 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 7.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[11] from at least 3 different EU Member States or

[11] 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.

	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.
Technology Readiness Level	Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to all of the following outcomes:

- Improved capabilities of European Police Authorities and other relevant security practitioners for a fast and flexible analysis of huge amounts of heterogeneous data through the application of robust and advanced tools, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Enhanced and modern analysis of heterogeneous data as well as training curricula that take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data, providing reports that can be used in court;
- The work of European Police Authorities in the area of fighting crime and terrorism is supported by big data analysis that is in accordance with data minimisation principles and high privacy standards, with clearly identified challenges, adequate models and scientifically validated technical options for tackling the challenge proposed and solutions developed that meet the challenge.

Scope: With the constant increase of technological developments, the processing of large datasets is inevitable for police work in today's digital world. As a wide range of products and services become digitalised and interconnected, Police Authorities need adequate technologies to properly detect and counter emerging threats. Big data analysis also provides invaluable opportunities to carry out investigations, identify suspects, reveal or anticipate crime patterns or links between previously unconnected events or actors. In particular, there is a continuous need for handling large, complex and unstructured datasets, in order to gather, normalise, process, connect, prioritise, visualise the data (including text, image, audio and video) in ways that facilitate the extraction of actionable intelligence, while ensuring interoperability between existing systems and standards in different Member States. Solutions to perform temporal and geospatial analyses are needed too. The successful proposal should have a clear strategy related to quality data sets to be used for training and testing. The innovation efforts should provide support to web-based data analysis that can facilitate e.g.

the fight against hate speech, human trafficking, terrorism or child sexual exploitation in an online environment. The work should include surface, deep and dark web.

Examples of relevant techniques include: examination of digitally captured signatures, identification of voice cloning and of deepfakes; detection and recognition of persons/objects/logos; speaker diarisation and identification; speech recognition and transcription into text; automatic classification of text based on risk factors; optical character recognition; named entity recognition; concept extraction, extraction of entities and relations between them in unstructured text; multimodal analytics, in order to discover insights and patterns in large volumes of data through clustering, as well as the identification of user communities and key actors in the social networks being formed online; automatic correlations among all available sources, as well as cross-checking, cross-matching and mapping information between different cases, i.e. cross-reference with existing records in databases of Police Authorities. Identification of perpetrators can also be enhanced by detecting their online behaviour and habits, e.g. which days/hours they are used to login/logout.

Taking advantage of these modern technologies will require Police Authorities to move away from business models based on data input to data evaluation. It will require robust and reliable information management structures that encompass all aspects from data collection to handling, evaluation, exploitation and data security. In particular, key principles such as data minimisation should apply to ensure that Police Authorities conduct data analysis in full compliance with fundamental rights and EU privacy standards. For example, it may be necessary to filter and reduce large datasets to what is relevant for operational support activities and in investigations, and/or apply methods such as differential privacy. Hence, all these efforts should also reconcile big data analysis and data protection, i.e.: explore challenges to conduct big data analysis in accordance with data minimisation principles and high privacy standards, propose possible models and scientific options to tackle the challenge, and develop solutions (digital tools) that meet the challenge, focusing on triage and clustering functions. Possibilities of assessing and preventing bias and discrimination as a result of big data analysis should be analysed too. The successful proposal should thus help framing the issue of big data analysis for Police Authorities, providing guidelines as well as operational tools to comply with EU data protection standards.

The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as create synergies with similar on-going security research projects from the Calls 2021-2022 on Fighting Crime and Terrorism in the area of modern information analysis, in order 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 the consortium deems it relevant in relation to the objectives of the research effort.

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.

Possibilities of coordination with related activities funded through the Internal Security Fund (such as the European Anti-Cybercrime Technology Development Association) and the Digital Europe Programme should be analysed too.

FCT02 - Improved forensics and lawful evidence collection

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[12] and 2 forensic institutes from at least 3 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. To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the two options (Option A and Option B), provided that the applications attain all thresholds. If projects use satellite-based earth observation, positioning, navigation

[12] 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.

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

- European Police Authorities, forensic institutes and other relevant security practitioners are equipped by modern means of chemical analysis (composition) in drugs aimed at facilitating the cross-matching of seized drugs to labs and the establishment of links between cases, including by developing protocols to quickly exchange information on new substances;
- Improved and uniform EU-wide approach for the collection of evidence regarding illicit drugs-related overdoses, that would allow for choosing adequate responses in countering the drug-related problems;
- Improved collection and availability of forensic evidence, that could be used in court by the authorities, in direct violence, kidnapping or human trafficking cases, as well as reinforced prevention of such cases thanks to sensors/kits that are reliable, lawful, fast and easy-to-use;
- Enhanced perception of citizens in public and private spaces that Europe is an area of freedom, justice and security.

Scope: Proposals are expected to address one of the following options:

Option A: A harmonised European approach is needed on the study of chemical analysis (composition) in drugs, to

1) facilitate the cross-matching of seized drugs to labs and the establishment of links between cases, including by developing protocols to quickly exchange information on new substances;

2) tackle forensic challenges related to illicit drugs-related overdoses.

The production of synthetic drugs in the EU is continuously expanding. The laboratories producing synthetic drugs are becoming more professional and versatile, resulting in an increased production and a greater flexibility in terms of which substances are produced, how they are produced and how/where they are sold.

On the one hand, criminal networks and criminals active in the production of synthetic drugs display a particularly high degree of specialisation. Thus, a modern and harmonised European approach to the analysis of the drugs composition would help to crossmatch seized drugs and illegal drugs markets to labs and make the links between cases, allowing a cross-border exchange of such evidence.

On the other hand, choosing appropriate responses that are likely to be effective in dealing with a particular drug-related problem requires a clear understanding of the problem, supported by the strongest available evidence. However, an obstacle in this process is the very limited or fully absent evidence, as it is the case in finding responses aimed at reducing overdose-related deaths. Namely, autopsies with full toxicology are underdeveloped in many Member States, making comparison at EU level difficult and aggregated numbers on overdose deaths not fully representative. Member States called to make this issue more comparable EU-wide. To this end, a modern chemical analysis of the drugs composition and a unified EU-wide approach would provide a significant support, also in view of commitments of the EU Drugs Strategy 2021-2025.

Option B: A reliable and easy-to-use detection of chemical submission drugs in beverages and urine.

GHB (Gamma-hydroxybutyrate) is one of the drugs known as “club drugs” or “date rape drugs”. Notably when mixed with alcohol, it has a depressant effect and causes drowsiness, rendering the person defenceless and unable to remember what happened. Sexual assaults facilitated by chemical submission drugs have a growing tendency in Europe. Thus, Police Authorities and forensic practitioners need modern methods and technologies that enable better prevention against and investigation of different forms of violence and assault supported by these drugs. To this end, the successful proposal should aim at developing wearable, reusable, portable sensors and/or kits that would provide a fast response, without the need for additional instrumentation, and would be easy to use by Police Authorities in the field (i.e., in places where citizens are more at risk of ingesting GHB drugs through drinks and beverages). Furthermore, such solutions should provide results that are reliable, safe and simple to interpret when looking for and collecting evidence of such drugs that can be used in court. Gender-related impacts as well as legal and ethical challenges of such solutions should be fully considered in the development process.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Similarly, coordination with projects funded under *HORIZON-CL3-2022-BM-01-03: Better, more portable and quicker analysis and detection for customs* and *HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials* would be welcome.

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.

FCT03 – Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [13] from at least 3 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.
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to some or all of the following outcomes:

[13] 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.

- Strengthened resilience of local communities against crime and radicalisation, lowered feeling of insecurity and improved law enforcing;
- Negative factors in local communities are identified early, possible threats are detected, and crime reporting is enhanced;
- Better recognition for community diversity within neighbourhoods, and tailored approaches to milieus including communities traditionally not engaging with statutory authorities resulting in comprehensive community empowerment;
- The interactions, and potential feedback between CP and alternatives to incarceration are explored;
- Identification and EU wide dissemination of validated community policing best practices;
- New methodologies, tools and adoption of technological support are developed; and
- Training curricula for Police Authorities are developed on community policing in non-homogenous local milieus with social complexities, including balancing of majority needs while recognising expectations of minorities and/or sub-groups.

Scope: Community policing (CP) is an integral part of policing focusing on cooperation with local community for better understanding challenges and the given group needs and meeting them. From both a theoretical and a practical point of view, three ways of delivering CP may be outlined: reactive, proactive, and co-active - based on community consultations and common actions. While performing such actions, police provides information, initiates and participates in programs to prevent crime and ensures the protection of citizens in cooperation with other institutions. CP aims to create opportunities for positive, mutually respectful interactions between civilians and the police, to increase citizens` trust and enhance the ability of police to enforce the law. To maximise the impact of CP actions, proposals should analyse its potential relations with introduction of innovative alternatives to imprisonment.

Nowadays, Police Authorities, while carrying out their duties to provide community security, are faced with numerous economic and demographic challenges. As a consequence, more efficient solutions, tools and methodologies are sought. First responders cope with growing communities, tighter budgets, and diverse, quickly evolving milieus in their areas of responsibility, regularly facing challenges that initial professional training could not prepare them for. Moreover, rapidly changing social, economic and political environment, both domestically and internationally, complicates these problems and fuels new tensions.

New approaches should cover internal review of Police Authorities' personnel training, possible change of attitudes and communication language, or countering existing misconceptions and biases. International exchange of validated best practices is encouraged. Proposals should eventually integrate societal findings, relevant new or already existing technologies and legal framework into a comprehensive CP model. The successful proposal should build on the publicly available achievements and findings of related previous national

or EU-funded projects. Activities proposed within this topic should address both technological and societal dimensions of CP in a balanced way.

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.

FCT04 – Increased security of citizens against terrorism, including in public spaces

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-04: Open topic

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [14] from at least 3 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. 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 5-7 by the end of the project – see

[14] 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.
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: Projects' results are expected to contribute to all of the following outcomes:

- Enhanced ability of security practitioners to identify and prevent emergent challenges in the terrorism-related topic under consideration;
- Harmonised and modern tools as well as procedures in the investigation of 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 European Police Authorities, as well as with international actors, in tackling the problem in question; and
- Training curricula for Police Authorities are developed 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 citizens against terrorism, including in public spaces, that are not covered by the other topics of Calls Fighting Crime and Terrorism 2021-2022, Call Fighting Crime and Terrorism 2023 and Call Fighting Crime and Terrorism 2024.

Adapted to the nature, scope and type 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. 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.

FCT05 – Organised crime prevented and combated

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-05: Crime as a service

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [15] from at least 3 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.
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to all of the following outcomes:

- European Police Authorities and policy makers are provided with a robust analysis of the evolution of the contemporary organised crime, its structure, role of hierarchy, membership in the organisation and subcontracting of specialised criminal services.
- Policy makers benefit from an analysis of the legal framework utilised for countering organised crime, in terms of the validity of the legal definitions and penal provisions adopted and their impact on the effectiveness of judicial verdicts;
- Methodology for the identification of the means of advertising, communication, marketing and money flows used for offering criminal services on the underground

[15] 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.

market is developed, as well as the set of respective prevention, investigative and policy countermeasures; and

- Improved knowledge within European security institutions regarding developments in the field of organised crime and prospects for the future.

Scope: The Crime-as-a-service (CaaS) model proliferates and becomes a prominent feature not only for the cybercriminal underground, but also for traditional criminals hiring specialised digital and financial services. Thus, availability of exploit kits and other services not only serves cybercriminals with low technical skills, but also makes the operations of mature and organised threat actors more efficient. Recently Malware-as-a-service (MaaS) offerings on the Dark Web increased, of which ransomware affiliate programs seem to be the most prominent.

The shape of the organised crime evolves, apart from traditionally closed, clandestine criminal structures, and investigators are increasingly confronted with modern, flexible, specialised and "multi-ethnic" organisations with a global operational range. As these groups seem not to work within permanent multi-layered structures but with various actors delivering on demand services, some of the organised crime characteristics might be subject to a review. Actors in the shadow economy while seeking to maximise their profit, take instant advantage of new ways of operations, exploring and benefiting from modern technologies and organisational schemes to achieve their goals, thus resulting in dynamic transformation of subject networks. The observed trend may be a challenge for the codified laws and definitions of organised crime as supposedly sealed off to outsiders and characterised by fixed and permanent cooperation. In order to enhance the fight against organised crime at the European level, there is a need for distinct research to gain comprehensive insight into the internal workings of modern organised crime structures and their marketplaces.

Coordination among the successful proposal from this topic as well as with the successful proposals under topics HORIZON-CL3-2023-FCT-01-06: *Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes* and HORIZON-CL3-2024-FCT-01-06: *Tracing of cryptocurrencies transactions related to criminal purposes* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

FCT06 – Citizens are protected against cybercrime

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes

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.

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [16] from at least 3 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.
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of modular toolbox for Police Authorities, facilitating gathering and processing of data relevant for cybercrime and cyber - enabled crime investigations;
- Detection of crypto-jacking, compromised registration forms, malware attacks and other cybercrimes perpetrated using cryptocurrencies;
- Development of training curricula, for Police Authorities, prosecutors, as well as judicial actors on major contemporary cybercriminal activities;
- Recommendations on public cybercrime awareness actions contributing to early detection and prevention;

[16] 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.

- Identification of best practices of international law enforcement and judicial cooperation networks; and-
- Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms.

Scope: While cyber-attacks, notably ransomware and distributed denials or services, are getting more sophisticated, law enforcement officers need to develop strategies to gain a comprehensive knowledge of the numerous elements contributing to the attack (Virtual Private Networks - VPNs, Bulletproof Hosting – BPH, Remote Access Trojans – RATs, botnets, Dark Web platforms, crypto-ransomware, Criminal Phone Banks, Pseudonyms, Advanced Persistent Threat groups – APTs, Internet infrastructure abuse (e.g. DNS), etc.). Having in mind that these are offered today in a form of *Crime-as-a-service* for anyone willing to pay, there is growing number of cases where authorities have to launch and conduct advanced inquiries. Investigators need timely access to relevant data and expertise of a different nature and belonging to different categories of stakeholders (e.g. other Police Authorities or Internet service providers). As geographical boundaries become irrelevant in the commission of crime, criminal investigations have to become cooperative, joint actions. It does not seem feasible for a comprehensive investigation of contemporary organised crime to be conducted by a single investigator or even a single force. This technical and organisational complexity together with the cross-border nature of cyberattacks requires cutting-edge investigative approaches, gathering a large range of expertise as well as trusted information sharing mechanisms across communities (including secured platforms). In addition, it is necessary to enhance cybercrime intelligence picture notably by enhancing reporting mechanism of cyber-dependent criminal activities. Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms, is necessary in order to enhance prevention and deterrence of these forms of cyber and cyber-dependent crime. Project should also investigate the legal background and identify any related shortcomings so lawful access and processing of subject data has a valid legal foundation.

Coordination among the successful proposals from this topic as well as with the successful proposal under HORIZON-CL3-2023-FCT-01-05: *Crime as a service* should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Call - Fighting Crime and Terrorism 2024

HORIZON-CL3-2024-FCT-01

Conditions for the Call

Indicative budget(s)[17]

[17] 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.

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[18]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-FCT-01-01	RIA	5.00	Around 5.00	1
HORIZON-CL3-2024-FCT-01-02	RIA	9.00	Around 4.50	2
HORIZON-CL3-2024-FCT-01-03	RIA	3.70	Around 3.70	1
HORIZON-CL3-2024-FCT-01-04	RIA	4.00	Around 4.00	1
HORIZON-CL3-2024-FCT-01-05	IA	6.00	Around 6.00	1
HORIZON-CL3-2024-FCT-01-06	IA	6.00	Around 6.00	1
Overall indicative budget		33.70		

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

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 years 2023 and 2024.

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

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

FCT01 - Modern information analysis for fighting crime and terrorism

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-01: Mitigating new threats and adapting investigation strategies in the era of Internet of Things

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	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [19] from at least 3 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. 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 5-6 by the end of the project – see General Annex B.

[19] 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.

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: Projects' results are expected to contribute to all of the following outcomes:

- Increased understanding of Police Authorities regarding the emerging (digital and especially physical) threats of the fast-developing environment of Internet of Things;
- Modern tools to tackle new and emerging forms of crime pertaining to the development of Internet of Things are provided to European Police Authorities and other relevant security practitioners, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data;
- Lawful access and exploitation of evidence in the environment of the Internet of Things are fortified;
- Best practices (legal, organisational, technical) to access and exploit Internet of Things in the course of investigation are strengthened, including by developing relevant tools and training materials.

Scope: Internet of Things (IoT) connects practically everything and makes everything more vulnerable as well. IoT devices increasingly benefit from the convergence and integration of technologies, such as machine learning, real-time analytics as well as 5G that will provide faster and more reliable connections for all devices.

There are a number of implications particular to IoT devices, which have been consistently highlighted by researchers and Police Authorities. For example, the vulnerability of IoT devices may be exploited by criminals who seek to collect personal data, compromise user credentials or spy on organisations or people. Furthermore, IoT devices may represent a threat that goes beyond the digital world, i.e. they may become an increasingly physical threat, since they find applications in, e.g., industry and infrastructure, as well as in building smart cities. Malevolent actions against connected devices with direct physical impact (e.g. car-to-car communication, hacking of vehicles, hospitals, nuclear plants) are also a growing concern.

Therefore, the successful proposal should help Police Authorities understand the implications of the fast-developing IoT environment in order to keep pace with the evolution of its applications, recognise and tackle the emerging (digital and especially physical) threats that this may pose.

At the same time, IoT proliferation will provide opportunities for the Police Authorities and other relevant security practitioners to collect a new range of data in relation with criminal activities. New investigating schemes are needed for Police Authorities to access and exploit

IoTs evidence, in compliance with EU values. To this end, the proposal should examine the extent to which, e.g., modern European vehicle models, smart TVs, private surveillance systems, virtual assistants or voice control systems can be considered as sources of evidence for the collection and analysis of data, as well as how such data can be used for deriving indicators of an imminent threat.

The research should assess legal, organisational and technical implications of IoT development in the context of investigations, including e.g. privacy issues, and propose strategies, including training materials, tools and path to standards that would foster "by design" a lawful access to relevant evidence.

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

The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as create synergies with similar on-going security research projects from the Calls 2021-2022 on Fighting Crime and Terrorism and on Increased Cybersecurity, in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Possibilities of coordination with related activities in the Digital Europe Programme[20] should be analysed too.

FCT02 - Improved forensics and lawful evidence collection

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-02: Open topic

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:

[20] REGULATION (EU) 2021/694 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

	The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[21] and 2 forensic institutes from at least 3 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. 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 5-7 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to all of the following outcomes:

- Improved European common forensics investigation capabilities, evidence collection and cross-border exchanges in the domain under consideration;
- Police Authorities and forensic institutes are provided with innovative, harmonised and modern tools and procedures for forensic applications in the investigation of the crime under consideration, in full compliance with applicable legislation on protection of personal data;
- Forensic practitioners and Police Authorities active in crime scene investigations are provided with modern and innovative training curricula in the forensic domain under consideration.

Scope: In the Open topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive forensic solutions for fighting crime and terrorism, that are not covered by the other topics of Calls Fighting Crime and Terrorism 2021-2022, Call Fighting Crime and Terrorism 2023 and Call Fighting Crime and Terrorism 2024.

[21] 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.

Adapted to the nature, scope and type 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. 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.

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

Research proposals should consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. When applicable, the successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects.

HORIZON-CL3-2024-FCT-01-03: Lawful evidence collection in online child sexual abuse investigations, including undercover

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.70 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 3.70 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[22] and 2 forensic institutes from at least 3 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.
Technology	Activities are expected to achieve TRL 5-6 by the end of the project – see

[22] 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.
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: Projects' results are expected to contribute to all of the following outcomes:

- Development of safer justice outcomes through an increased understanding of the EU-wide legal aspects of online investigations, including undercover, in the area of child sexual abuse;
- Improved understanding of the EU-wide legislative hurdles that impact (undercover) investigations in this area;
- Modern and robust methods at the European level are proposed at all steps of an investigative process in this area, overcoming various types of biases and obstacles to the collection of evidence that is admissible in court and respects the dignity, privacy, protection of personal data and anonymity of victims;
- Forensic practitioners, Police Authorities and other relevant security practitioners active in online (including undercover) child sexual abuse investigations benefit from innovative guidelines, manuals, education and training curricula.

Scope: The use of online undercover investigation techniques is an important asset for Police Authorities in infiltrating the networks of sexual abusers of children. These methods have proven very effective in understanding offender behaviour and interaction of online service providers, and have ultimately facilitated the shutting down of communication channels used by these offenders, as well as their prosecution. An increasingly important need for Police Authorities' activity in these spaces is the ability to effectively infiltrate particularly dangerous online groups of offenders, while making sure that the evidence obtained will be admissible in court. EU values and fundamental rights shall stay in the core of any future measures. Research in this area should tackle legislative hurdles to collecting evidence in online, including undercover, investigations of child sexual abuse, leading to guidelines and manuals that would make the capability available across the EU to target these offenders more effectively. The results of this research topic (training, manuals guidelines) should be shared among all European Police Authorities, notably via CEPOL, provided that the Agency opts out from applying for funding under this topic. The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as create synergies with similar on-going security research projects from the Calls 2021-2022 on Fighting Crime and Terrorism in the area of digital forensics and countering child sexual abuse, in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Since the use of undercover agents online could be beneficial in other crime areas too, particularly in counter terrorism, analysis of possibilities for the developed approaches to be adapted to these other crime areas would be welcome. Special care needs to be given to ethics and fundamental rights protection throughout the research and the solutions proposed. 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.

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.

FCT03 – Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-04: Radicalisation and gender

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: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [23] from at least 3 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.

[23] 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 5-6 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved understanding of motivation of women and girls for supporting extremist ideologies, such as grievance and stigmatisation;
- Improved understanding of the role of masculinity in men and boys' motivation for the support of extreme ideologies;
- Better understanding of the group dynamics at play during processes of radicalisation, including factors for factionalism and potential splinters in terrorist organisations;
- Development of strategies aimed at enhancing the use of motivation factor in detection, prevention and de-radicalisation efforts;
- European Police Authorities, Prison Authorities, social care workers, teachers and other P/CVE practitioners benefit from modern and validated tools, skills and training curricula to identify early symptoms of radicalisation;
- Identification and assessment of best practices that are transferable across Member States improving and developing modules and trainings, strengthening adaption of local community policing in diverse communities; and
- Design girls and women's empowerment approaches through legal, financial and/or cultural means aimed at tackling the root causes of radicalisation and extremism.

Scope: Terrorism resulting from radicalisation and violent extremism is a serious threat to European security. Part of the complexity of these phenomena lies in the fact that there is neither a single pathway to radicalisation nor a single terrorist profile. Support of extremists is an effect of individual clusters of psychological, personal, social, economic and political reasons. From a gender perspective, women's radicalisation and involvement in violent extremist groups remain relatively under-researched, poorly understood and possibly characterized by misconceptions about women's exclusion from decision-making processes, as well as their significant underrepresentation in bodies countering the phenomena. In situations of conflict and violence, women are often seen as passive, victims, subordinate and maternal, while these could be assumptions reinforcing gender stereotypes. In order to improve understandings of radicalization and gender we need to study how and why gender norms appear as an increasingly contested area of politics with strong mobilizing power. What role gender norms and equality policies play in stabilizing and destabilizing social and

political order, and how ideas and norms about gender equality make people react, mobilize and engage politically, at present, in the past and in the future. The entry point for prevention and de-radicalisation efforts are local communities, which are both stakeholders and partners of the law enforcement in this process. Activities aimed at youngsters and adults have to be gender sensitive, and research has to deliver tailored advice and solutions adequately, and proportionately addressing all critical issues.

Community policing with its multidisciplinary approach seeks the cooperation of local communities and the broad range of public authorities in its efforts of building safe environments. However, those efforts should recognise not only cultural, social and economic diversity of the milieus, but as mentioned above also be gender sensitive. The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as seek to exploit potential synergies with the successful proposal(s) funded under HORIZON-CL3-2023-FCT-01-03*: New methods and technologies in service of community policing and transferable best practices*, and HORIZON-CL2-2024-DEMOCRACY-01-05: *Gender-roles in extremist movements and their impact on democracy*.

Moreover, the EU Counter-Terrorism Agenda adopted in 2020 outlines that Radicalisation Awareness Network (RAN) will identify best practices and approaches of community policing and engagement to build trust with and among communities, thus research under this topic should also build upon the work done by RAN. 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.

FCT04 – Increased security of citizens against terrorism, including in public spaces

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-05: CBRN-E detection capacities in small architecture

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.
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:

	The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [24] from at least 3 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. 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.
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: Projects' results are expected to contribute to all of the following outcomes:

- Improved vulnerability assessments by law enforcement and local managers of public spaces by detection of chemical, biological, radiological, nuclear and explosive (CBRN-E) threats in the public spaces and flow of public transport, in order to provide broader situational awareness to practitioners in the field;
- Enhanced planning capabilities of security practitioners and policy-makers due to the access of new data and identification of potential vulnerabilities connected to the design/refurbishment and improvement of different public spaces;
- Recommendations are provided for further improving safety and security-by-design approach to public spaces and mass transportation systems;
- Improved training of Police Authorities in collaboration with different public and private actors (e. g., crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services, security managers, private security organisations, civil society groups etc.) to enhance their preparedness to attacks on public spaces; and

[24] 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.

- Enhanced modelling capabilities for security practitioners and policy-makers due to the identification of potential new vulnerabilities and data available, and improved support to planning of respective resources and activities.

Scope: Public spaces such as squares, sport venues, shopping districts, places of worship, and mass transport systems have been the target of terrorist attacks causing significant loss of lives and causing societal insecurity. Means to carry out such attacks range from sophisticated, and well-planned scenarios including several coordinated attackers using explosives and firearms, to low-cost, low-tech attacks making use of common products. Today specific urban furniture like benches, bus shelters, flower boxes, etc. already have double functions controlling access to protected areas, which answers to some of the low-cost attacks. The next logical step seems to expand their functions further and adopt new functionalities to better respond to the terrorist threats, such as for CBRN-E ones. The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects, as well as seek to exploit potential synergies with the successful proposal(s) funded underHORIZON-CL3-2024-BM-01-05: Detection and tracking of illegal and trafficked goods.

In recent years, in some pilot actions some street furniture, including bins and bus shelters have become *smart* as they have been equipped with environmental sensors, wireless modules, or microcontrollers becoming part of the IoT infrastructure, and one of the components of the future smart cities. Proposals should focus on exploitation and integration of existing sensors within the public space small architectures. Traditional sensors and surveillance platforms like the Automatic Number-Plates Recognition (ANPR), cameras or image analysis systems are not in the scope of this topic unless their integration with new sensors is considered, and the added value of networked systems demonstrated. Proposals should present relevant challenges and opportunities for future applications of CBRN-E detection capacities in small architecture, including prospects of scalability, real-time processing, and cooperation of networked systems.

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 the consortium deems it relevant in relation to the objectives of the research effort.

FCT06 – Citizens are protected against cybercrime

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-06: Tracing of cryptocurrencies transactions related to criminal purposes

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.
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: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [25] from at least 3 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.
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
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: Projects' results are expected to contribute to all of the following outcomes:

- The attractiveness of use of cryptocurrencies by criminals and terrorists is limited, with better tractability of cryptocurrency transactions;
- Lawful tools and methods for Police Authorities to better trace virtual currency transactions related to criminal activities;

[25] 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.

- Recommendations are provided for better regulation of the cryptocurrencies market as well as for better regulation of the exchange of transnational information on funds transfers, harmonizing and promoting standards to enhance the tracing of money flows in the context of criminal investigations; and

- Modern training curricula for Police Authorities, Prosecutors, as well as judicial actors are developed on tracing, seizing and handling cryptocurrencies in the course of investigation.

Scope: Cryptocurrencies are a widely used method by criminals, including terrorists, to transfer or conceal funds due to their anonymity, ease of use and lack of international borders and restrictions (exactly same aspects that make use of traditional bank routes difficult for them). With the raise of crime-as-a-service market, and growth in the number of connected transactions, use of cryptocurrency as one of the money laundering typology better tracing of cryptocurrency transactions is crucial to keep the ground in the fight against crime and terrorism. On top of it all, clandestine cryptocurrency activities are increasingly facilitated by new developments such as high privacy decentralised exchanges, which while used by perpetrators frustrate the efforts of Police Authorities to detect and recover criminal assets as well as to prevent fraudulent transactions. The future of cryptocurrencies and the extent to which criminals and terrorists will use them will depend on factors such as anonymity, future regulation, law enforcement activities and security of the systems. Innovation should explore these considerations and propose mitigation measures, from legal, organisational, and technical perspectives (including the development of tools and relevant trainings to enhanced tractability of cryptocurrencies transactions. Proposals should also propose cooperation model(s) and tools for the exchange of information between relevant authorities.

The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects. Coordination among the successful proposal from this topic as well as with the successful proposals under topic HORIZON-CL3-2023-FCT-01-06: *Crime as a service* 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 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 the consortium deems it relevant in relation to the objectives of the research effort.

Destination - Effective management of EU external borders

This Destination addresses, among other, objectives identified by the **Security Union Strategy**[26] as well as the border management and security dimensions of the **New Pact on Migration and Asylum**[27] and the **Strategy on the Schengen Area**[28]**.** As such, topics included under the Destination aim at ensuring strong European land, air and sea external borders. This includes: developing strong capabilities for checks at external borders hence safeguarding the integrity and functioning of the Schengen area without controls at the internal borders; compensating the absence of intra-EU border checks; being capable to carry out systematic border checks, including identity, health and security checks as necessary, while facilitating the travel of bona fide travellers and respecting rights and possible vulnerabilities of individuals; providing integrated and continuous border surveillance, situational awareness and analysis support; combating identity and document frauds; supporting future technology for the European Border and Coast Guard; supporting the interoperability and performance of EU data exchange and analysis; supporting better risk detection, incident response and crime prevention; improving European preparedness to, and management of, future rapidly evolving changes; and updating our maritime security management including migration, trafficking as well as search and rescue capabilities. The capabilities built by research and innovation in this Destination would clearly be relevant to be better prepared for potential future challenges to European internal security and crises as the ones in Ukraine in 2022.

Taking into account the central role of the European Border and Coast Guard Agency (Frontex) in defining capability requirements, and approving the capability roadmap for the European Border and Coast Guard, and in addition to the contribution from the Member States, the Agency will be closely associated with, and will assist the European Commission in drawing up and implementing, relevant research and innovation activities. Research should follow the indications of the long-term components of the capability roadmap of the European Border and Coast Guard once adopted (expected in 2023).

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.

Research should also consider how future management of borders can develop protection of human rights, and how it can facilitate protection of refugees.

This research will also contribute to the implementation of the European Border Surveillance System (EUROSUR) and the development of tools and methods for Integrated Border Management.

---

26 COM(2020) 795 final.
27 COM(2020) 609 final.
28 COM(2021) 277 final.

Regarding maritime security, the topics under this Destination will also support the implementation of the relevant actions under the capability development, research and innovation area of the EU Maritime Security Action Plan[29], and the Joint Communication on a Stronger EU Engagement for a Peaceful, Sustainable and Prosperous Arctic[30]. Research activities will therefore enable better security and management of EU maritime borders, maritime critical infrastructures, maritime activities and transport, contributing as well to a better performance and cooperation on coast guard functions. Research and innovation in the area of maritime security will also support the development of future capabilities for the protection of sea harbours and related sea lines of communication including entry/exit routes. The objective of maritime security research activities in this regard covers prevention, preparedness and response to expected and unexpected events including anthropogenic and natural disasters, accidents, climate change as well as threats such as terrorism and piracy, cyber, hybrid and chemical, biological, radiological and nuclear and explosive (CBRNE) ones. The EU Maritime Security Research Agenda lays down in this regard specific areas to address, including cybersecurity, interoperability and information sharing, autonomous systems, networking and communication systems and multi-purpose platforms. Specific EU maritime security legislation[31] also emphasises maritime passenger transport, and the threats to passengers. Innovative and more efficient capabilities for the security of maritime passenger transport could therefore also be a useful area of research.

Regarding security in the movements of goods across external borders, research will address requirements identified by the European Commission and EU customs authorities and should contribute to capabilities for detecting illegal activities both at external border crossing points and through the supply chain. EU customs authorities face increasing volumes of commerce, trade and traffic of goods, as well as having a range of tasks to fulfil besides security. International smuggling has the potential to become more sophisticated and/or increase in the coming years and decades, and could be facilitated by cybercrime. Criminal networks may exploit potential weaknesses of global supply chains, transport and logistics to pursue illicit trade and other crimes. At the same time, threats and hazards that may need to be detected in the flow of goods are very diverse and often need different sensors and technologies to be detected (from chemical, biological, nuclear, radiological and explosive material to drugs, firearms, money, waste, trafficked wildlife, cultural goods, etc.). Hence, customs need innovation to enable detection and to ensure security without at the same time disrupting or unnecessarily hampering trade flows. Capabilities built through research will contribute to the implementation of the EU Customs Union action plan to reinforce customs risk management and effective controls. Capabilities include those on threat detection; automated controls and detection that reduce the need to open or stop containers, packages, baggage or cargo; decision support; portability of control solutions; and technologies to track cross-border illicit trade.

---

29 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf

30 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0027&from=EN

31 Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

Furthermore, in order to accomplish the objectives of this Destination, additional eligibility conditions have been defined with regard to the active involvement of relevant security practitioners or end-users.

Successful proposals under this Destination are invited to cooperate with other EC-chaired or funded initiatives in the relevant domains, such as the Networks of Practitioners projects funded under H2020 Secure Societies work programmes, the Knowledge Networks for Security Research & Innovation funded under the Horizon Europe Cluster 3 Work Programme, the Community of European Research and Innovation for Security (CERIS) or with other security research and innovation working groups set-up by EU Agencies.

Furthermore, successful proposals under this Destination should be complementary and not overlap with relevant actions funded by other EU instruments, including projects funded by the Digital Europe Programme as well as the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), while maintaining a focus on civilian applications only.

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; and to prepare the uptake of the research outcomes.

Proposals involving earth observation are encouraged to make use primarily of Copernicus data, services and technologies.

This Destination will develop knowledge and technologies that may be taken up by other 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), that will enable exploitation of research results and final delivery of the required tools to security practitioners.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:

"Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Improved security (as well as better cost- and energy- efficient management) of EU land and air borders, as well as sea borders and maritime environment, infrastructures and activities, as well as for the EU external civilian security, against accidents, natural disasters and security challenges such as illegal trafficking, piracy and potential terrorist attacks, cyber and hybrid threats;

- Improved border crossing experience for travellers and border authorities staff (including customs, coast and border guards), while maintaining security and monitoring of movements across air, land and sea EU external borders, supporting the Schengen area, reducing illegal movements of people and goods across those borders and protecting fundamental rights of travellers, both EU citizens and Third Country Nationals;

Improved customs and supply chain security though better prevention, detection, deterrence and fight of illegal activities involving flows of goods across EU external border crossing points and through the supply chain, as well as through better interoperability, minimising disruption to trade flows.

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) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-BM-01	23.90		23 Nov 2023
HORIZON-CL3-2024-BM-01		24.00	20 Nov 2024
Overall indicative budget	23.90	24.00	

Call - Border Management 2023

HORIZON-CL3-2023-BM-01

Conditions for the Call

Indicative budget(s)[32]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[33]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-BM-01-01	IA	7.00	Around 7.00	1
HORIZON-CL3-2023-BM-01-02	RIA	4.90	Around 4.90	1
HORIZON-CL3-2023-BM-01-03	RIA	6.00	Around 3.00	2
HORIZON-CL3-2023-BM-01-04	IA	6.00	Around 6.00	1
Overall indicative budget		23.90		

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.

[32] 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 years 2023 and 2024.

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

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.

BM01 – Efficient border surveillance and maritime security

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-01: Capabilities for border surveillance and situational awareness

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 7.00 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 7.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: 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. 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).
Legal and	The rules are described in General Annex G. The following exceptions

financial set-up of the Grant Agreements	apply: 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). [34].
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased border surveillance capabilities, better performing and more cost-efficient, with data and fundamental rights protection by design;
- Better surveillance of border areas, supporting fight against illegal activities across external borders, as well as safety of people and operators in the border areas, including favouring border crossings through border crossing points;
- More efficient and more flexible solutions (including for relocation, reconfiguration and rapid deployment capabilities) than physical barriers to deter and monitor irregular border crossings outside border crossing points.

Scope: External borders of the European Union and of the Schengen area, ranging from those closer to the Mediterranean to the Nordic Countries external land borders, present different border surveillance challenges. These differences may lead to difficulties in efficiently monitoring them, deterring illegal activities across the external borders, as well as trafficking of human beings and exploitation of irregular migration that avoid border crossing points.

Furthermore, the border surveillance capabilities' needs along borders may change in time, often just within a year or a season, and/or allow to respond and adapt within a relatively short notice. Solutions should hence allow re-orienting capacity and resources accordingly (through physical portability and/or other approaches).

Cooperation for surveillance along borders requires compatibility and interoperability among legacy and planned systems. Proposed solutions should allow higher interoperability cross-border among EU and Associated Countries practitioners, cross-systems and across the multiple authorities.

[34] 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

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

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): networked deployable, and possibly mobile, semi-autonomous surveillance towers; IoT and advanced mesh connectivity; Virtual and Augmented Reality for enhanced C2 and situational awareness; integrated wide area RPAS management; advanced sensors for geolocalisation; passive, low-energy systems; artificial intelligence.

Equipment and technologies enabling border surveillance should contribute to cost and energy efficiency, limit their environmental impact and be more and more sustainable once operational in the future. This may be addressed, for example, by integrating opportunities of circular economy, self-sustained equipment, lower emissions and/or environmental footprints.

The proposed solutions should include, by design, the protection of fundamental rights such as privacy, and/or the application of privacy-enhancing technologies. They should also ensure secure data collection, access, encryption and decision support processes.

EU and Member States authorities should plan to take up the results of the research, should it deliver on its goals and when compatible with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects. In particular, proposals should build on achievements and findings or relevant recent EU-funded civil security research projects, as well as projects from topic *HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support*, and other relevant 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.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap when available; and on the engagement with the Agency during the implementation of the project. This perspective should be considered and planned when drafting proposals. Proposals should foresee that Frontex will observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the border and coast guard community. Cross-community and cross-authority synergies within civil security can be an asset, for

example in relation to combat crime and terrorism (i.e. across external borders) and Disaster-Resilient Society (regarding natural hazards and disasters).

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-02: Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.90 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 4.90 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [35].

[35] 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: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased capabilities to detect, classify, inspect, assess and neutralise UXO at sea;
- Improved safety and security for maritime economic operators and for EU citizens.

Scope: A large amount of Unexploded Ordnance (UXO), estimated by experts in the tens of thousands of tons, lay in European seas and often close to European shores. Most of this material dates back to World War I and World War II. Estimates for the timing of material corrosion suggest that much of this material is likely to be an increasing safety risk in the next 10 years. And this would happen while coasts, shores and seas have more and more value for economic and civilian activities, ranging from seafood production to communications, transport, trade and sustainable energy production. UXO hence represents a substantial safety risk for economic operators at sea, and citizens, as well as for the environment.

UXO also represents a security risk, as some of this dangerous material is relatively easily retrievable and could be misused in illicit, including criminal and terrorist, acts. These security threats could be linked directly to maritime security and infrastructures (to deny or ransom a port, for example), or be moved towards other illicit acts.

Roles and responsibilities to map, identify, assess, inspect, retrieve and/or neutralise UXO vary among Member States, allocated to private operators, local and regional governments, national governments, and/or the military that carry out civilian tasks.

Current capabilities on mapping, identifying, assessing, inspecting, retrieving and/or neutralising UXO still largely use human operators, and increased use of automated and/or unmanned systems would be desirable for efficiency and safety reasons.

The proposed project should improve civilian capabilities on:

a) enabling existing knowledge (mapping and integrating data from historical maps and more recent data, including reports from sea operators); comparative analysis of legislation, roles and responsibilities in Member States;

b) detecting UXO on and below the marine sediment/seabed, in order to detect also buried objects;

c) identifying, classifying, assessing (identifying chemical and material aspects; sensing levels of corrosion);

d) inspecting and handling (grab and manipulate UXO under water, from intact shells to chunks to small parts; collect and recovery);

e) neutralising and disposing (containment of chemical spill overs and possible explosions).

Especially for proposing new solutions for the capabilities areas a) to c) described above, proposals should take into account and build on existing information produced and compiled by previous EU projects that carry out regular work on environmental risks of hazardous submerged objects such as UXO[36].

Research projects should consider results and recommendations from the European Commission's 2022 "Study on underwater unexploded munitions: final report"[37].

Research projects should consider, build on and not duplicate previous research or findings of previous operational work, including but not limited to research by other Framework Programmes projects and/or other EU projects, including those funded by the EU Maritime and Fisheries Fund, by the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), or by JPI Ocean. Relevant work by civilian national or regional projects[38], or by regional organisations (such as, for example, NATO/CMRE Research Centre).

For objectives in the capabilities areas d) and e) described above, proposals should focus on the solutions that address the civil needs and challenges of UXOs (not necessarily deriving from mine countermeasures), with regard to civil resources and engaging civil stakeholders.

Indeed, the involvement of civilian stakeholders, beyond civilian authorities, such as operators on sea, is strongly encouraged. The project should focus on civilian capability gaps and needs, rather than capabilities that are better addressed by defence instruments and tasks.

Proposed solutions should be compatible or interoperable with legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

Proposed solutions that would improve energy efficiency and environmental impact aspects of current UXO risk mitigation operations (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): sonars and other sensors; UxVs/AUVs; on-board analytical capabilities for material samples; hydroacoustic profiling; artificial intelligence for detection and classification; wing tows from ships; system of systems architecture.

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.

---

36 See for example Sea-Dumped Chemical Munitions – Baltic Marine Environment Protection Commission, Helsinki Commission (HELCOM).

37 https://data.europa.eu/doi/10.2926/5356

38 Such as, for example PROBANNT, CONMAR, or AMMOTRACE.

Synergies within civil security can be an asset, for example with Fighting Crime and Terrorism (regarding combating organised crime and terrorism) and Disaster-Resilient Society (regarding environmental contamination).

BM02 – Secured and facilitated crossing of external borders

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-03: Beyond the state-of-the-art "biometrics on the move" for border checks

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: The following additional eligibility criteria apply: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [39].
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Updated, European-based, knowledge and development on robust biometrics technologies that could be used for recognition (identification and verification) of people crossing external EU borders, demonstrating a clear advancement beyond the current state-of-the-art;
- Maximisation of travellers' experience and of security reassurances, minimising handling of personal data and maximising accuracy, reliability and throughput of the recognition process;
- Contribution to improving the operational response capacity of the EBCG at border crossing points and to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Biometrics are one of the most usable and most reliable ways to validate the identity of an individual. Biometrics that are traditionally used in the context of border controls include fingerprints and 2D facial images; other biometrics are also used for identity management outside the European Union, or at national level, such as iris; and further others are used in other applications in the private sector and in consumer market.

As for many other technologies, applications of biometrics to improve capabilities in civil security, such as in the border management or law enforcement sectors, may have higher requirements than applications in the consumer market. This applies to the requirements on reliability, usability, scalability, throughput and strict minimization of risks to personal data protection and fundamental rights (including the elimination or minimisation of any risk of bias or discrimination).

Research should assess and develop the fit-for-purpose border management of biometric identification modalities beyond fingerprints and facial images, and/or innovative modalities of acquisition of those and other biometrics. Proposed projects should particularly investigate biometrics modalities that currently do not offer satisfactory performance (in terms of

[39] 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

accuracy, reliability, usability, minimisation data protection risk and risk of bias etc.) but potentially offer significant advantages over existing solutions in the short or medium term for applications in a border checks context.

Any innovation in biometrics shall imply clear improvements on acquisition, processing and validation, compared to the state-of-the-art, "on-the-move" (i.e. while the travellers are moving and without cooperation from them), contactless and with stand-off biometric capturing from long-distances (ideally, but not mandatorily, more than 10 meters), and/or of when multiple travellers cross borders, on foot or inside the same vehicle. The solutions should also take into account the different nature and scenarios of BCP operations (e.g. open-air conditions, night, time, time constraints, space constraints, etc).

The solutions should comply with the requirements of current and foreseen EU large-scale IT systems on borders and visa (e.g. the Entry/Exit System), as well as with interoperability frameworks between EU large-scale IT systems on borders, visas, asylum and migration, as well as on police and judicial cooperation.

The proposed solutions should comply with data protection by design and by default, meet robust fundamental rights impact assessment frameworks as well as apply privacy-preserving and privacy-enhancement by design solutions. Developed solutions could indeed help reduce the amount of biometric data needed to achieve improved reliability of identification, including by acquiring and using less personal data compared to the state-of-the-art.

The project should also study the stability over time of collected biometrics, and if and how it would be possible to "re-use" collected biometrics in a secure and privacy-friendly manner, for the same purposes and according to allowed uses, collected biometrics, and avoid collecting the same biometrics multiple times.

The proposed solution(s) should address modular integration with health checks – such as in the case of pandemics – as well as checks on people's temperature. At system-level, emphasis should be given to automated border check for the purpose of guiding travellers on-the-move while performing the seamless biometric acquisition. Systems should also be compatible with policies and measures typically introduced during pandemics (e.g. the use of facemasks and social distancing).

The proposed solutions should include automated decision support systems for the biometric recognition process suggesting to the end-users (border checks operators) which procedure, technology or database can be used without infringing rights of travellers.

The developed solutions need to comply with the Ethics Guidelines on Trustworthy AI (2019)[40].

EU border authorities in the consortia should plan to take up the results of the research, assuming the project delivers on its goals and is compatible with applicable legislation, using the financial support of the Border Management and Visa Instrument (BMVI).

[40] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): 3D facial images, contactless friction-ridge biometrics (i.e. fingerprint, palmprint and finger-knuckle-print), iris recognition from long distances, palm vein, periocular biometrics, novel algorithms embedding artificial intelligence as well as advanced hardware components like sensors, traveller tracking systems for high-quality on-the-move biometric acquisition, safe single wavelength or multispectral light sources (for the illumination of subjects) and document verification subsystems.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other relevant recent EU Framework Programmes projects on security research, and projects funded under *HORIZON-CL3-2021-BM-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff* and *HORIZON-CL3-2022-BM-01-02: Enhanced security of, and combating the frauds on, identity management and identity and travel documents*.

Proposals should delineate concrete, clear and convincing plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment in operational context of border checks) at national and EU level, should the research deliver on its goals.

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 when available; and on the engagement with the Agencies during the implementation of the project. This perspective should be considered and planned when drafting proposals. Proposals should foresee that Frontex and of eu-LISA will observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the border and coast guard community.

The funded projects will likely have the opportunity of exploiting the core capabilities of the "Border Management Innovation Centre" (BoMIC), Frontex's future collaborative physical space for testing, demonstration, simulation and assessment of border-check prototype systems, processes and procedures with a focus on human-machine interaction and emulation of real operational environments.

BM03 – Better customs and supply chain security

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials

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.
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: The following additional eligibility criteria apply: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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

[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

	classified and sensitive information of the General Annexes.

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

- Increased interoperability of existing (and foreseeable upcoming) customs control equipment at tactical level, multi-supplier, multi-authority and cross-border;
- More efficient and quicker availability, for EU customs practitioners, of reference data (such as spectra) on threats and dangerous and/or illicit materials;
- Building capabilities for a more harmonised European application of customs controls based on risk management and trade facilitation.

Scope: European customs, as all operators and citizens, also work in our digitalised and interconnected world of equipment, systems, and data. On the one hand, this opens opportunities to harness their capacity to facilitate trade while protecting the security and safety of citizens and benefiting the EU's economy. On the other hand, the proliferation of equipment, system and data, often from different suppliers and in different versions, may also present challenges in terms of interoperability and an efficient management of flows of goods across the external borders of the Custom Union. Furthermore, the strategy of the "European custom union acting as one" implies that other authorities beyond customs use that same equipment. It also means that equipment, including mobile one, is shared among Member States to increase cooperation and collaboration on checking flows of goods across European borders. Finally, it equally means that standards and technical specifications for customs control equipment are harmonised.

Another challenge for European customs control capabilities is the rapid availability of, and rapidly shared, data references for (new) threats and illicit materials.

All this calls for research and innovation for solutions that prepare and increase the interoperability of customs control equipment and data at "tactical" level, in terms of multi-authority, cross-border, multi-supplier interoperability as well as linkages among Member States and Commission systems, and the more rapid availability and sharing of libraries of reference data for target substances or materials. There is room for innovation to improve access to updated spectra (or other formats or references) of target substances and materials when they appear; easily make them available to customs' devices; and improve data for libraries.

The solution(s) proposed under this topic should define the requirements and way forward to enable and enhance the interoperability of customs control equipment and of data used in different Member States and/or by different authorities at national level, as well as Commission systems.

The proposed solution(s) should address how to make libraries of data references on target substances and materials more rapidly available and shared with authorities; to update and

share them faster and securely; to enable quicker tackling of illegal substances and materials, either innovating current approaches or designing altogether new approaches for reference libraries.

EU customs authorities should take up the results of the research in the framework of the Customs Union "acting as one", with the support of the Customs Control Equipment Instrument (CCEI). The CCEI will enable not only the possibility to establish harmonisation through common standards and technical specifications but will offer access to actively fund equipment across the Member States to fulfil these common standards.

The proposed solution should include privacy enhancing techniques to allow the sharing of tools without the sharing of data beyond what is strictly necessary. Leaking or compromising personal data should be avoided in the transfer of tools or models.

Improving energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): blockchain/DLT, artificial intelligence; spectroscopy, data fusion.

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

Call - Border Management 2024

HORIZON-CL3-2024-BM-01

Conditions for the Call

Indicative budget(s)[42]

Topics	Type of	Budgets (EUR	Expected EU contribution per	Indicative number

[42] 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 years 2023 and 2024.

	Action	million) 2024	project (EUR million)[43]	of projects expected to be funded
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-BM-01-01	IA	6.00	Around 6.00	1
HORIZON-CL3-2024-BM-01-02	IA	6.00	Around 6.00	1
HORIZON-CL3-2024-BM-01-03	IA	6.00	Around 6.00	1
HORIZON-CL3-2024-BM-01-04	IA	6.00	Around 6.00	1
Overall indicative budget		24.00		

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.

BM01 – Efficient border surveillance and maritime security

Proposals are invited against the following topic(s):

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

HORIZON-CL3-2024-BM-01-01: Interoperability for border and maritime surveillance and situational awareness

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.
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: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [44].
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] 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: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased border surveillance capability, better performing and more cost-efficient, with data and fundamental rights protection by design;
- Improved surveillance and situational awareness of sea borders, but also of maritime infrastructures as harbours and commercial and civilian maritime security, including in key areas such as the Arctic;
- Improved multi-level, multi-authority and cross-border (among Member States and Associated Countries practitioners) collaboration thanks to better interoperability of sensing, analysis and C2 systems.

Scope: Authorities performing surveillance of maritime borders and maritime wide areas use a range of technologies, and receive a range of information, to monitor wide areas, detect threats or crises, and respond to them. However, these inputs are not always merged into common command-and-control (C2) systems that can inform rapid decision-making.

The proposed solution(s) should allow improved interoperability (at both back-end and front-end levels), independently of the supplier of the equipment, and ideally interchangeability that enables exchange of information among authorities that use different systems.

The proposed solution(s) can include the design of open architecture C2 systems, including open standards for APIs and bias-free data models.

The proposed solution(s) should enable simultaneous connection of different sensors (or of different data, or of different assets, depending by the module) by different suppliers, the flexible tasking and monitoring of surveillance assets like RPAS, and the visualization and manipulation of the data in a single user interface in a seamless way. This will support practitioners to exploit their technology stack in an agnostic way.

The proposed solution(s) should allow for seamless connectivity between C2 systems from different authorities, and at different coordination levels; include cybersecurity measures and information access segregation capabilities; include concepts of operation, standard operating procedures and common lexicon for joint operations using interoperable systems through the proposed solution(s).

While the project will mainly focus on enabling capabilities through interoperability and interchangeability, proposals that in the process aim at advancing certain technological components, and integrating them into the solution, are welcome.

Assuming the project delivers on its goals, EU and Member States authorities should plan to take up the results of the research when compatible with applicable legislation using the financial support of the Border Management and Visa Instrument (BMVI).

Improving energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): open architecture; user interface and experience; artificial intelligence; UxV; wide-area and long-endurance RPAS and integrated, wide-area RPAS cooperative tasking and management; remote sensors (such as LIDAR or FMCW) on UxVs; vessels-as-sensors; advanced mesh connectivity; automated analysis of abnormal or non-cooperative vessels' behaviour; Virtual and Augmented Reality; standardized mission data models for RPAS tasking and monitoring, ; and/or over-the-horizon detection technologies.

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 also clearly demonstrate how they complement and do not overlap with actions undertaken in the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), while ensuring the civilian focus and application.

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.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap when available; and on the engagement with the Agency during the implementation of the project. This perspective should be considered and planned when drafting proposals. Proposals should foresee that Frontex will observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Synergies within civil security can be an asset, for example with Disaster-Resilient Society and Fighting Crime and Terrorism.

BM02 – Secured and facilitated crossing of external borders

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-BM-01-02: Advanced user-friendly, compatible, secure identity and travel document management

Specific conditions	
Expected EU	The Commission estimates that an EU contribution of around EUR 6.00

contribution per project	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: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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.

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

- Improved capabilities to validate breeder and identity documents as well as ICAO Type 1 and Type 2 digitalised travel documents;

[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

- Improved compatibility among tools for verification of travel documents and identity, while guaranteeing not sharing (beyond what's strictly necessary) or compromising personal data;

- Enhanced integration with EU current or planned architecture(s) for digital identity frameworks;

- Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Authentication of documents is relevant for border management, immigration or visa applications. Furthermore, it could also be relevant to combat other illicit activities, such as financial fraud. Facilitation of travel across external EU borders went and is further going through remarkable developments thanks to subsequent technological generations, and updated procedures and regulatory frameworks. From automated border control gates to "no-gate" solutions, and to "seamless travel"; from secure documents, to digitalised travel documents, and to "dematerialised travel documents" and "digital wallets". All to ease border crossing for travellers, while maintaining border security against illicit or irregular crossings and protecting fundamental rights. This topic aims at exploring and developing enhanced capabilities for securely managing digitalised travel documents used for travel across external borders.

The proposed solution should be compatible with planned or possible future EU highly digitalised travel documents formats and travel facilitation systems, and with applicable ICAO current and upcoming schemes. The proposed solutions should be compatible or interoperable with relevant existing digitalised travel documents systems. The proposed solutions should also respect fundamental rights such as privacy and protection of personal data, apply privacy by design of the application and use privacy-enhancing technologies.

The operational applicability focus should be on highly digitalised travel documents and "digital identity management" used for travel across external borders. However, the research should include enhancing the security of breeder documents, which risk being "weak links" when they are used to obtain genuine, secure travel documents.

The proposed solution should include techniques (including those to increase the robustness against attempts to falsify biometric data) to allow sharing of results from the tools, and share as few data used by the tool as possible to return those results (in order to increase data protection and minimize data leak risks). Leakage or compromising of personal data should be avoided in the transfer of tools or of their results.

The proposed solution should ensure secure data collection, access, encryption and decision support for those in relevant roles in the border management processes. Full encryption at transit and rest should be ensured, while enabling fuzzy searches on all metrics of the documents' data.

The proposed solution should include an automated decision support system that helps the work of operators and suggests to end-users (such as border authorities' staff) which process and which database/tool can be legally used with, or by, a certain technology or database.

The developed solutions need to comply with the Ethics Guidelines on Trustworthy AI (2019)[46].

Should the project deliver on its goal and be compatible with applicable legislation, EU and Member States authorities should plan to take up the results of the research with the support of the Border Management and Visa Instrument (BMVI).

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects. In particular, proposals should build on achievements and findings of relevant recent EU-funded civil security research projects, including those funded under *HORIZON-CL3-2022-BM-01-02: Enhanced security of, and combating the frauds on, identity management and identity and travel documents*.

Proposals should delineate concrete and clear plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment in operational contexts) at national and EU level, should the research deliver on its goals.

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 when available; and on the engagement with the Agencies during the implementation of the project. This perspective should be considered and planned when drafting proposals. Proposals should foresee that Frontex and of eu-LISA will observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Synergies across authorities and across communities (such as border management, customs, law enforcement communities) within the civil security sector will be an asset, for example with Fighting Crime and Terrorism (regarding combating crime involving identity fraud).

HORIZON-CL3-2024-BM-01-03: Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy

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.

[46] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

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: 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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [47].
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Improve assisted border crossing control systems, coordinated between border, customs and security controls;
- Allocate more efficiently border check resources, maintaining security while minimising time and hassle for crossings and false positives;
- Allocate flexibly border check resources, when and where needed, depending on changing needs (for example seasonally, and/or in the case of roll-on-roll-off ferries);

[47] 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

- Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Growth of international travel and mobility (which will likely return to, and increase to a level above, the pre-COVID-19 pandemic levels), the scarcity of resources, and the need to ease border crossings while maintaining security of the Schengen area, make reliable risk assessments and border checks prioritisation important. Border practitioners in some Member States are assessing feasibility, reliability and acceptability of optimised border controls using risk-based management.

The solution(s) proposed under this topic should allow easier and more flexible allocation and change of resources in border checks, for example to meet seasonal peaks. A possible use case is that of roll-on-roll-off ferries. That situation may generate long queues for border and security checks, while often being seasonal. A proposed solution should help perform border checks, as well improve the speed for detecting threats in vehicles, such as weapons and explosives, without people coming out of vehicles and without slowing down (dis)embarkment off or onto roll-on-roll-off ferries.

In any case, the proposed solution(s) should consider both the travellers and the goods accompanying them.

Higher leveraging of risk management in border crossing practices has the potential to also decrease and minimise the use of personal data and the risk for violating fundamental rights. The project should integrate strong ethical, legal and acceptability assessment to ensure that, on the other hand, the risks of bias (such as on ethnicity or gender) and discrimination of risk mitigation is minimised.

Collaboration with international stakeholders in the field of transport and transport safety in the air, maritime and rail contexts is encouraged.

Should the project deliver on its goal and be compatible with applicable legislation, EU and Member States authorities should plan to take up the results of the research with the support of the Border Management and Visa Instrument (BMVI).

The proposed system should ensure secure data collection, access, encryption, and decision support processes. Full encryption at transit and rest should be ensured, while enabling fuzzy searches on all metrics of the documents' data.

The system should include automated decision support systems that suggest the end-users which process and database/tool can be legally used using a certain technology.

Solutions should be compatible or interoperable with legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

Improving energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): risk assessment methods, data fusion, sensors, artificial intelligence.

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

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex), including basing on the EBCG Capability Roadmap when available, and engage with the Agency during the implementation of the project. This perspective should be considered and planned when drafting proposals. Proposals should expect a key role of Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

The involvement of Police Authorities[48] is encouraged, as well as synergies with relevant topics of the Fight against Crime and Terrorism Destination.

BM03 – Better customs and supply chain security

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-BM-01-04: Detection and tracking of illegal and trafficked goods

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.
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: This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member

[48] 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.

	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. 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).
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [49].
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Contributing to development of fully automated customs control checkpoints;
- Enhancing detection capabilities for customs security, while facilitating trade.

Scope: European customs need improved capabilities that allow bettering and automatically detecting from traces; interpreting images from scanned cargo; interpreting data; tracking goods; and/or identifying anomalies that support the detection of threats, smuggling or illicit trade eliminating or minimizing disruption to the trade flow. The proposed system should hence advance and/or combine as much as possible the components of detection, tracking and risk-based anticipation.

On detection, the proposed solution(s) could include trustworthy algorithms for recognition that minimise false positives and biases. Proposed research could include, for example, image (shape) recognition and interpretation, and/or a trace detection approach

[49] 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

On tracking, the research can propose and explore, for example, technologies for improved traceability of goods and items that could be illicitly trafficked using non-invasive markings.

On risk-based anticipation, the proposed solution(s) can leverage automated image recognition and interpretation capability coupled with data analytics, such as using advance cargo information in order to anticipate and detect security risks prior to goods' arrival at the EU external borders.

The research project can test one or more specific use cases, such as (non-exhaustive examples): art; cultural goods; waste and other environmentally risky material, including radioactive ones; valuables; and/or dangerous items either assembled or disassembled.

Improving energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): scanning (vision), detectors/"sniffers" (traces), nanotechnology, blockchain/DLT, artificial intelligence.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent 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 in the framework of the Customs Union "acting as one", with the support of the Customs Control Equipment Instrument (CCEI).

The involvement of Police Authorities[50] is encouraged, as well as synergies with relevant topics of the Fighting against Crime and Terrorism Destination.

[50] 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.

Destination - Resilient Infrastructure

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:*"[…] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructure operators […]"*

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Ensured resilience of large-scale interconnected systems infrastructures and the entities that operate them in in case of complex attacks, pandemics, natural and human-made disasters, or the impacts of climate change;
- Upgraded systems for resilience of the operators and the protection of critical infrastructure to enable rapid, effective, safe and secure response and without substantial human intervention to complex threats and challenges, and better assess risks ensuring resilience and open strategic autonomy of European infrastructures;
- Resilient and secure smart cities are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity.

The capabilities built by research and innovation in this Destination would clearly be relevant to be better prepared for potential future challenges to European internal security and crises as the ones in Ukraine in 2022.

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) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-INFRA-01	14.40		23 Nov 2023
HORIZON-CL3-2024-INFRA-01		12.20	20 Nov 2024
Overall indicative budget	14.40	12.20	

Call - Resilient Infrastructure 2023

HORIZON-CL3-2023-INFRA-01

Conditions for the Call

Indicative budget(s)[51]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[52]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-INFRA-01-01	IA	5.00	Around 5.00	1
HORIZON-CL3-2023-INFRA-01-02	IA	9.40	Around 4.70	2
Overall indicative budget		14.40		

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.

51 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 years 2023 and 2024.

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

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.

INFRA01 – Improved preparedness and response for large-scale disruptions of European infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 government entities responsible for security, which could include civil protection authorities, at national level from at least 3 different EU Member States. 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. 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). In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, or security, namely to protect and

	to preserve the confidentiality of risk assessments and of the vulnerabilities of critical entities of Member States, participation is limited to legal entities established in Member States only. Proposals including entities established in countries outside the scope specified in the call/topic/action will be ineligible.
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: 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). [53].
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: Projects' results are expected to contribute to all of the following outcomes:

- Tools for EU Member State authorities and operators for the assessment and anticipation of relevant risks to the provisions of essential services are identified;
- The cooperation between authorities of EU Member States is facilitated by providing solutions for data exchange and joint cross-border risk assessments;
- Simulation tools are developed for large-scale exercises to test the resilience of operators and of specific sectors, and related training courses are designed;
- Measures by Member State authorities to facilitate risk assessments by operators are identified, including the assessment of dependencies on different sectors and cross-border interdependencies;
- Provide common European guidance and support for the drafting of their resilience plans in order to meet all the provisions of the proposed CER-Directive: risk analysis, domino

[53] 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

effects, cross-sector and cross-border analysis, standardised plans, educational and training tools;

- An all-hazards framework is created to support Member States in ensuring improved concepts and instruments for the anticipation of risks to entities that provide essential services, resulting in an improved preparedness and response against disruptions of key sectors in the EU and enhanced resilience of the EU internal market.

Scope: The EU Security Union Strategy for 2020-2025, Counter-Terrorism Agenda for the EU and the Cyber Security Strategy stress the importance of ensuring resilience in the face of various risks. The livelihoods of European citizens and the good functioning of the internal market depend on the reliable provision of services fundamental for societal or economic activities in many different sectors. Those services often are reliant upon one another, thus disruptions in one sector can generate severe and long-lasting effects on the provision of services in others.

Member States hold the primary responsibility in ensuring that operators who use critical infrastructures to deliver such services (hereafter: 'operators') comply with applicable rules and have the necessary support to ensure their own resilience and as part of a complex system of interdependencies. On EU-level, there has been a revision of certain legislation aiming at the minimum harmonisation of such rules, such as the [proposals] for a directive on the resilience of critical entities (CER) and the directive on measures for high common level of cybersecurity across the Union (NIS-2). In combination with sectoral EU-legislation and policies on resilience (e.g. the proposal for a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows), this provides a comprehensive framework that needs to be put in practice.

"Facilitating strategic cooperation" refers to the necessity for public authorities of the Member States to be able to exchange information, in a secure way, on the risk assessments of their critical entities as well as their resilience. "Critical entities" is the specific term used in the proposed CER directive to designate those entities that will be identified by the Member States under the directive. Pursuant to the directive, in particular of its articles 1 and 5, the identity of the critical entities will be classified. In the performance of the project, project participants will interact directly with Member States authorities responsible for risk assessment and analysis of the vulnerabilities of their critical entities. Pursuant to the proposed directive, the confidentiality of the critical entities (and of their vulnerabilities) shall be ensured and protected.

Proposals under this topic should support the competent authorities of Member States to identify and develop the most suitable tools, solutions and strategies to ensure the resilience of key sectors and thus facilitate the implementation of [related/ future] EU legislation.

Applicants should focus on delivering solutions that can be used by the competent authorities of EU Member States, to support their task in overseeing the resilience of key sectors in line with relevant EU rules. Such solutions should enhance their ability for cooperation and communication, conducting large-scale risk assessments (including the cross-border

dimension), developing best practices for exercises and dedicated complex training modules. The proposals should address the development of improved concepts and instruments for the anticipation and management of strategic risks, strengthening governance framework and enhancing coordination between different authorities.

It is recommended that proposals develop concrete tools to support all-hazard analysis by integrating domain specific risk assessment and allowing to manage interdependencies phenomena among different sectors and Member States. Possible examples are virtual reality tools, dashboards, complex training and serious gaming modules or other instruments to be used and that currently may not exist on such scale.

Proposals should aim to cover the largest possible number of sectors described in the respective Annexes of the [proposals for a] directive on the resilience of critical entities (CER[54]) and the directive on measures for high common level of cybersecurity across the Union (NIS-2[55]).

Participation of at least 3 government authorities, from 3 different EU Member States, responsible for resilience on national level and/ or for overseeing operators is mandatory. The inclusion of associations representing private or public operators in specific sectors, or across sectors on EU- or national level, is encouraged.

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

Projects are expected to outline how results are fed into the work of relevant Commission expert groups – [for example the Critical Entities Resilience Group (CERG) and the NIS-2 Cooperation Group] – and to explore synergies with the actions undertaken by relevant EU agencies.

HORIZON-CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.70 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 9.40 million.

[54] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities (COM(2020) 829 final.

[55] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final.

Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: 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). The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 infrastructure operators, which could include civil protection authorities, at national level from at least 3 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.
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: 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). [56].
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Support is provided to the resilience of operators against cyber and non-cyber threats in specific sectors;

[56] 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

- A reliable state-of-the-art analysis of physical/cyber detection technologies and risk scenarios is created, in the context of an operator in a specific sector in sectors that have not yet been covered by previous research projects;

- Strengthened cooperation against natural or human-made threats and subsequent disruptions of infrastructures in Europe, allowing for operational testing in real scenarios or realistic simulations of scenarios with specific regard to disruptions in a specific sector of critical entities;

- Improved situational awareness, preparedness and governance by the implementation of effective solutions that enhance detection and anticipated projection of a determined threating situation, as well as implementation of prevention, preparedness/mitigation, response, and recovery types of intervention;

- Significant reduction of risks and exposures to anomalies or deliberate events on cyber-physical systems, or on complex and critical infrastructures/systems;

- Enhanced preparedness and response by definition of operational procedures of operators as well as public authorities considering citizen's behaviour/reaction and societal impact in case of disruption in a specific sector.

Scope: The operational environment in which operators operate has changed significantly in recent years. Security research and innovation related to infrastructure resilience has been following a sectorial approach in order to increase the resilience. This approach to critical infrastructure resilience is needed that as it reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures.

A disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also potentially in other Member States or across the entire EU.

With more and more infrastructure systems being interconnected, a stronger focus on the systemic dimension and complexity of attacks and disruptions by cyber or physical means needs to be applied. As such, not only interdependencies within one type of infrastructure (or closely related types) can be taken into account. The risk landscape is more complex in the recent years, involving natural hazards (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents).

Physical disruptions of the activities of operators active in these sectors have possibly serious negative implications for citizens, business, governments, in the environment and endanger the smooth functioning of the internal market. Therefore, operators should be equipped with the best possible means to be able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies.

Another important issue is to have in place efficient cybersecurity measures to block the access to critical infrastructures. A possible project focusing on the protection of critical infrastructures against such threat should consider gaps and vulnerabilities that need to be identified and overcome (e.g. protection of drinking water supply systems from high chemical levels, nuclear facilities, etc.).

Therefore, the successful proposal, following a sector-based approach and identifying a specific priority sector, should work on how to increase the combined cyber and non-cyber resilience operators. It should do so by orienting itself on sectors that have not been covered in previous research, out of the list of sectors described in the respective Annexes of the of the [proposals for a] directive on the resilience of critical entities (CER) and the directive on measures for high common level of cybersecurity across the Union (NIS-2) and thus contribute to enhancing the overall resilience on EU-level, in line with the EU Security Union Strategy.

The proposal should orient itself on the policy shift from protection towards resilience and thus focus on operators acting in the internal market, rather than only on physical or digital assets. This includes concepts of wider business continuity, as well as logistics and supply-chains. Proposals should also focus on the development of a more effective resilience plan conception method, which shall support operators to draft their resilience plans according to the provisions of the CER and NIS-2 Directives [proposals]. The resilience plan conception method should include risk analysis, domino effects analysis, cross-sector and cross-border analysis, standardised plans etc. In addition, this method could include measures on adequate protection, measures on prevention, response, mitigation, and recovery from the consequences of incidents, protection of classified (e.g. the proposal for a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows) or sensitive information and measures that ensure adequate employee security management.

The main practitioners in this topic should come from private or public operators, meaning organisations and enterprises that use critical infrastructure to deliver services, vital for the functioning of society and the internal market. Consortia that will include MS public entities would be considered as an asset. Competent authorities of MS in charge of resilience and/ or overseeing operators in one or more sectors are also encouraged to join the consortia of applicants.

If the infrastructure includes processing of personal data, the proposal should consider including a risk assessment or privacy impact of individuals and society.

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

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.

Applicants are encouraged to explore and demonstrate synergies with the work conducted in the European Reference Network for Critical Infrastructure Protection (ERNCIP), as applicable.

Call - Resilient Infrastructure 2024

HORIZON-CL3-2024-INFRA-01

Conditions for the Call

Indicative budget(s)[57]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[58]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-INFRA-01-01	IA	6.20	Around 6.20	1
HORIZON-CL3-2024-INFRA-01-02	RIA	6.00	Around 6.00	1
Overall indicative budget		12.20		

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.

[57] 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 years 2023 and 2024.

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

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.

INFRA02 – Resilient and secure urban areas and smart cities

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-INFRA-01-01: Resilient and secure urban planning and new tools for EU territorial entities

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.20 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 6.20 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 local or regional government authorities from 2 at least 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. 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 6-8 by the end of the project –

Readiness Level	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: 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). [59].
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: Projects' results are expected to contribute to all of the following outcomes:

- Evaluation of the resilience of an urban and peri-urban environment, identification of weaknesses and recommendations for changes to organizational processes;
- Creation of new tools and cost-efficient security upgrades of urban infrastructures with possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities;
- Improved efficiency of the security forces and emergency services (police, firefighters, paramedics ...) for the benefit of the European citizens and residents;
- Promotion of best practices, creation of EU sovereign trusted decision support tool/solution and spreading of effective tools and capabilities across entities in different EU territories despite their size and location.

Scope: European territories are developing into more connected and complex systems of different services and infrastructures empowered by technologies and growing digitisation. This change in urban areas in Europe, brings new opportunities but also new threats for the authorities and their relationship with the citizens and residents. It is therefore critical for the resilience of our urban areas and for their citizens' wellbeing that those services are trusted and secure.

The classical large-scale infrastructures have a long tradition of implementing the principles of Safety-by-design and Security-by-design when planning their assets. However, with more

[59] 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

and more infrastructures on the local level becoming vulnerable, security research can support their protection with new approaches in 'Security-by-design'. In view of limited budgets of many local administrations, improved knowledge as well as innovative security upgrades and processes for existing urban infrastructures equipped with advanced connectivity technologies and cooperative systems could be explored.

EU territories, despite their size and location, suffer from a lack of dedicated EU sovereign and trusted tools in order to enhance the coordination of local first responders and to improve security coverage, such as the preparation of operational staff, field intervention and predictive tools. Even though some complicated tools already exist, it is clear that there is no generic, cost effective and easy to use solutions for local authorities. Therefore, there is a need for creation of new tools that are designed in a simple manner and deployed in an effective way.

Resilient and secure urban planning tools for the development of holistic approaches that network the different organizational levels, sensor and communication levels and data rooms are very pertinent. These tools should assess the resilience of urban and peri urban territories, identify weaknesses and recommend changes to organizational processes, sensors and communication infrastructure. The secure urban and rural living spaces, technical solutions, organizational levels, and data rooms must be more closely linked. There is a clear need for a development of tools for recovery strategies and proactive foresight for urban and peri urban environments. The tactical tools should include modelling of urban centres and rural areas, predictive tools, improved global situational awareness and day-to-day planning and crisis management (e.g., simulation, training).

A minimum of 2 local authorities from 2 at least different Member States are required to join the consortia of applicants. The proposals should include a high level of confidence in data management and sharing, provide solutions on cybersecurity issues and take on board new type of threats. The proposed solutions should suggest trusted shared architectures, trusted data collection, secure computation on the data and management processes, modelling capabilities, hypervisor supporting global situational awareness with open and trusted API's, trusted data processing engines and, e.g., artificial intelligence tools. If the tools include processing of personal data, it should consider including a risk assessment or privacy impact of individuals and society.

The testing and/or piloting of the tools and solutions developed in a real setting and the participation of one or more relevant local authorities is an asset; regardless, actions should foresee how they will facilitate the uptake, replication across setting and up-scaling of the capabilities - i.e. solutions, tools, processes et al. – to be developed by the project.

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-CL3-2024-INFRA-01-02: Advanced real-time data analysis used for infrastructure resilience

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.
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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 infrastructure operators, which could include civil protection authorities, at national level from at least 3 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. 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 5-6 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: 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). [60].

[60] 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: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis (including big data) by public and private actors via secured and trusted platforms and interconnected systems where the collaboration follows clear legal and political frameworks;
- Tools and processes for facilitating stakeholders efforts to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected events risks in advance by allowing for the analysis of various data sources (e.g. audio, video, social media, web-content, spatial information, sensor or machine generated data);
- Fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains;
- Interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment in order to allow for remote on-scene operations considering citizen knowledge;
- Increased cyber-resilience of industrial xG networks and cloud data covering specific infrastructure domains
- Improved ability to map in real-time the source(s) of risk factors that could endanger the networked infrastructure supported by Earth Observation and geolocation data. If the analysis includes processing of personal data, it should consider including a risk assessment or privacy impact of individuals and society.

Scope: Today's society is more interconnected than ever before. Telecommunication networks, transport networks, aviation, energy, water grids, finance are the backbone of today's society. Due to their exceptional complexity and size, infrastructure networks pose a specific challenge when it comes to identifying different risks, either cyber or physical. Especially in the cyber-domain, many intrusions or attacks remain unnoticed or are detected relatively late. Technological developments in areas like machine learning for analytics, user interfaces as well as storage applications have the potential to improve related capabilities.

Modern urban environments and interconnected infrastructures create constantly big amounts of data. In addition, other sources can be exploited to support the identification and analysis of risks to infrastructures. Therefore, research on enhanced risk anticipation through real-time

data analysis has the potential to lead to useful tools to enhance preparedness (contingency plans, scenario-based exercises, allocation of resources, etc.).

Resilience of smart cities is marked by a set of specific requirements taking into account most notably aspects from the integration considering user centred approaches as well as social and ethical aspects of Industrial Internet of Things (IIoT), AI/ Machine Learning approaches for real-time data analytics, ensuring transparency, sufficient knowledge and their operational challenges in this area.

While the availability of larger amounts of data from different sources offers potential to improve the identification of possible risks to infrastructures, it also increases the demand for fast and resilient analytical tools. There is a need to filter information to identify data that is relevant as an indicator for risks and - given the large number of different forms of cyber-attacks or intrusions - also a need to prioritise and decide according to the degree of danger they present. This implies the need for matching data in the appropriate context and verifying the source with a view of ensuring that only relevant data is analysed, thus avoiding false results. Faster identification and localisation of hazardous agents and contaminants inside the infrastructure networks is a key to allow for quick response, inform and involve citizens and residents as well as avoid large-scale damage of any incident. Such identification capabilities can be deployed as part of the infrastructure and integrate with the systems public authorities use to make sure information is available as soon as possible. Furthermore, it is crucial to develop methods for better cooperation between different actors to ensure a common understanding and interpretation of data and to provide interactive tools for exchange and visualisation for decision support. Cooperation between different public and private actors is essential in this regard.

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

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.

Destination - Increased Cybersecurity

Proposals for topics under this Destination should set out a credible pathway contributing to the following impact of the Strategic Plan 2021-2024: "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture.

All proposals of projects under this Destination should be complementary and not overlap with relevant actions funded by other EU instruments, including the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), while maintaining a focus on civilian applications only.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-CS-01	50.70		23 Nov 2023
HORIZON-CL3-2024-CS-01		50.90	20 Nov 2024
Overall indicative budget	50.70	50.90	

Call - Increased Cybersecurity 2023

HORIZON-CL3-2023-CS-01

Conditions for the Call

Indicative budget(s)[61]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[62]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-CS-01-01	IA	23.00	4.00 to 6.00	4
HORIZON-CL3-2023-CS-01-02	IA	15.70	2.00 to 4.00	4
HORIZON-CL3-2023-CS-01-03	RIA	12.00	4.00 to 6.00	2
Overall indicative budget		50.70		

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

61 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 years 2023 and 2024.

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

	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.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 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.
Indicative budget	The total indicative budget for the topic is EUR 23.00 million.
Type of Action	Innovation Actions
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains;
- Cloud infrastructures vulnerabilities mitigation;
- Secure integration of untrusted IoT in trusted environments;
- Use of Zero-Trust architectures;
- Trust & Security for massive connected IoT ecosystems & lifecycle management;

- Secure interoperability and integration of systems;
- AI-based automation tools for cyber threat intelligence;
- Secure infrastructure, secure Identities and usability for a security chain covering communication, data collection, data transport, and data processing.

Scope: The evolution of our interconnected society brings multiple layers of cloud, edge computing, and IoT platforms that continuously interact with each other. Yet this always-connected ecosystem populated with potentially vulnerable entities requires advanced, smart and agile protection mechanisms to manage the security and privacy of individual components throughout their lifecycle and of overall systems. The complexity of such interconnected environments underlines the need for the proactive and automated detection, analysis, and mitigation of cybersecurity attacks in cloud, at the edge, for OT, IoT deployments, and in application domains such as, for example, smart cities. Integrating end-to-end security and user-centric privacy in complex distributed platforms requires work to address security threats and vulnerabilities over the entire platform ecosystem.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS02 –Privacy-preserving and identity technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 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 15.70 million.
Type of Action	Innovation Actions
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [63].

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

- Improved scalable and reliable privacy-preserving and identity management technologies for federated and secure sharing and for processing of personal and industrial data and their integration in real-world systems;
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solutions;
- Privacy by design;
- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with DATA Topics of Horizon Europe Cluster 4). Also, contribution to the promotion of eID Regulation compliant European solutions;
- Research and development of self-sovereign identity management technologies and solutions;
- Provide resource efficient and secure digital identity solutions for Small and medium sized enterprises (SME);
- Strengthened European ecosystem of open-source developers and researchers of privacy-preserving solutions;
- Usability of privacy-preserving and identity management technologies.

Scope: Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine-learning methods process medical and behavioural data in order to find causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data, potential privacy risks (e.g. attribute disclosure or membership inference) and identity compromises pose threats to individuals, society and economy, which hamper further developing data spaces involving personal data. Likewise, there are similar challenges for the exploitation of non-personal/industrial data assets that may compromise the opportunities offered by the data economy. Advanced privacy-preserving technologies such as, for example, cryptographic anonymous credentials, homomorphic encryption, secure multiparty computation, and differential privacy have the potential to address these challenges. However, further work is required to ensure and test their applicability in real-world use case scenarios.

[63] 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 security of any digital service or the access to data is based on secure digital identities. The eID Regulation provides the legal framework on which to build technological solutions that address the user needs concerning their digital identity. With regards to personal data, it is also important to develop self-sovereign identity solutions that give users complete control on their personal data and use.

Proposals should address usability, scalability and reliability of secure and privacy-preserving technologies in supply chain and take integration with existing infrastructures and traditional security measures into account. They should further take into account, whenever needed, the legacy variation in data types and models across different organizations. The proposed solutions should be validated and piloted in realistic, federated data infrastructures such as, for example, European data spaces. They should ensure compliance with data regulations and be GDPR compliant by-design. Open-source solutions are encouraged.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and, where relevant, end-users. The use of authentication and authorisation infrastructure framework tools developed for data spaces, and notably with the European Open Science Cloud, could be considered. Participation of SMEs is strongly encouraged. Legal expertise should also be added to ensure compliance of the project results with data regulations and the GDPR.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS03 - Secured disruptive technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 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.
Indicative budget	The total indicative budget for the topic is EUR 12.00 million.
Type of Action	Research and Innovation Actions

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

- Security-by-design concept and resilience to adversarial attacks;
- Inclusion of context awareness in machine learning in order to boost resiliency.

Scope: Proposals received under this topic will address the security of AI systems, in the line with the following considerations. The availability of very large amounts of data, together with advances in computing capacity, has allowed the development of powerful Artificial Intelligence applications (in particular Machine Learning and Deep Learning). At the same time, concerns have been raised over the security, robustness of the AI algorithms (including AI at the edge), including the risks of adversarial machine learning and data poisoning. Thus, it is important to promote security-compliant AI algorithms, leading to possible certification schemes in the future.

Proposals should demonstrate awareness of the EU approach on Artificial Intelligence[64], such as the proposed Artificial Intelligence Act.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

Call - Increased Cybersecurity 2024

HORIZON-CL3-2024-CS-01

Conditions for the Call

Indicative budget(s)[65]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[66]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-CS-01-01	IA	32.00	4.00 to 6.00	6
HORIZON-CL3-2024-CS-01-02	RIA	18.90	4.00 to 6.00	4

64 A European approach to artificial intelligence: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

65 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 years 2023 and 2024.

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

Overall indicative budget		50.90		

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.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-CS-01-01: 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 4.00 and 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.
Indicative budget	The total indicative budget for the topic is EUR 32.00 million.
Type of Action	Innovation Actions
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: 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). [67].

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

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

Scope: Software is at the foundation of all digital technologies and, as such, at the core of IT infrastructures, services, and products. Current software development prioritises fast deployment over security, which results in vulnerabilities and unsecure applications. Security engineering, both at the software and hardware levels, must be integrated in their development. Whilst a great portion of the software and hardware used in the EU is developed outside the European Union, it should comply with the security requirements within the EU. The EU should be able to rely on software and hardware that can be verified and audited as to their security. In particular, the potential security implications of using open-source software and hardware, and security auditability in that context, should be further explored. Software is subject to continuous update, so the security posture cannot be assessed once and for all, hence methods and tooling to perform continuous assessments of security are needed. In addition, security and privacy regulations also evolve, having to be factored in compliance approaches.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS02 - Cryptography

Proposals are invited against the following topic(s):

[67] 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-CL3-2024-CS-01-02: Post-quantum cryptography transition

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 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.
Indicative budget	The total indicative budget for the topic is EUR 18.90 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: 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, associated countries, OECD countries. Proposals including legal entities which are not established in these countries will be ineligible.

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

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

Scope: The advent of large-scale quantum computers will compromise much of modern cryptography, which is instrumental in ensuring cybersecurity and privacy of the digital transition. Any cryptographic primitive based on the integer factorization and/or the discrete logarithm problems will be vulnerable to large-scale quantum-powered attacks. The digital

data/products/systems that derive their security ultimately from the abovementioned primitives will be compromised and must be upgraded - including their replacement when needed- to quantum-resistant cryptography. The massive scale of this foreseen upgrade shows that preparations are needed today in order to widely implement the relevant mitigations in the future. Many companies and governments cannot afford to have their protected communications/data decrypted in the future, even if that future still seems distant. There is a need to advance swiftly in the transition to quantum-resistant cryptography.

Post-quantum resistant cryptographic algorithms should be deployable in a dynamic manner in order to quickly react to new quantum computer developments. Recommendations for post-quantum cryptography have already been published, but have to be maintained up-to-date, Proposals received under this topic should contribute to developing coordinated European recommendations for the transition to post-quantum cryptography across the EU.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

Destination - Disaster-Resilient Society for Europe

Proposals involving earth observation are encouraged to primarily make use of Copernicus data, services and technologies.

Proposals are encouraged also to coordinate with ESA relevant activities, especially those undertaken under the Science for Society element of the FutureEO programme (https://eo4society.esa.int). Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:

"Losses from natural, accidental and human-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness and resilience and improved disaster risk management in a systemic way."

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Enhanced exploitation of the latest scientific results (e.g., from research programmes and institutions) and integrated technologies (e.g. Earth observation, in situ data collection, advanced modelling, AI) into enhanced understanding of high-impact hazards and complex compound and cascade events and improved prevention, preparedness to mitigation, response, and recovery tools;

- Enhanced understanding and improved knowledge and situational awareness of disaster-related risks by citizens, empowered to act and consider innovative solutions, thus raising the resilience of European society;

- More efficient cross-sectoral, cross-disciplines (including SSH), cross-border coordination of the disaster risk management cycle and governance (from scientific research to prevention, preparedness to mitigation, response, and recovery, including knowledge transfer and awareness of innovative solutions) from international to local levels;

- Enhanced collaboration, interactions and cross-discipline dialogue and networking between the scientific community, research institutions and programmes (e.g., HE, ESA scientific activities, national science programmes, FutureEarth RIS-KAN) and first and second responders through dedicated networking and collaboration actions fostering a faster transfer of results from science into practice;

- Support of harmonised and/or standardised and interoperability of guidelines / protocols / tools / technologies in the area of crisis management, natural disasters and CBRN-E;

- Strengthened capacities of first responders in all operational phases related to any kind of natural and human-made disasters so that they can better prepare their operations, have access to enhanced situational awareness, have means to respond to events in a

faster, safer and more efficient way, and may more effectively proceed with victim identification, triage and care;

- Improved impact forecasting capability and scenario building for enhanced stress testing of critical entities and adaption of protection and resilience-enhancing activity accordingly;

- Improved ability to rescue and manage the first phases of emergencies that take into account extreme climatic events and/or geological hazards that may threaten urban areas (e.g. interface fires, floods, earthquakes, tsunamis, volcanic eruption etc.).

All proposals of projects under this Destination should be complementary and not overlap with relevant actions funded by other EU instruments, including the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), while maintaining a focus on civilian applications only.

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) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-DRS-01	27.50		23 Nov 2023
HORIZON-CL3-2024-DRS-01		24.00	20 Nov 2024
Overall indicative budget	27.50	24.00	

Call - Disaster-Resilient Society 2023

HORIZON-CL3-2023-DRS-01

Conditions for the Call

Indicative budget(s)[68]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[69]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-DRS-01-01	RIA	8.00	Around 4.00	2
HORIZON-CL3-2023-DRS-01-02	RIA	6.00	Around 6.00	1
HORIZON-CL3-2023-DRS-01-03	IA	4.00	Around 4.00	1
HORIZON-CL3-2023-DRS-01-04	RIA	6.00	Around 6.00	1
HORIZON-CL3-2023-DRS-01-05	RIA	3.50	Around 3.50	1
Overall indicative budget		27.50		

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.

[68] 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 years 2023 and 2024.

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

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.

DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-01: Improving social and societal preparedness for disaster response and health emergencies

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 organisations representing citizens or local communities, practitioners (first and/or second responders), and local or regional authorities and private sector from at least 3 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.

	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).

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

- Identification of different factors in inequality and ways to communicate with vulnerable groups, of individual, organisational, and systemic resilience factors and pathways to support these, and of ways to address vulnerabilities in acute crisis as well as during prevention, in order to elaborate an interconnectedness of resilience and vulnerability;

- Improvement of populations health literacy and basic understanding of how medicine and vaccines work and how they are developed and produced;

- Improved crisis communication through increased awareness and risk perception regarding bio security, identification of challenges for and limits of communication strategies and interventions regarding different vulnerable groups and approaches to address these, elaborating of ways for resolving barriers for crisis communication: interlinguality, interculturality, intersemiotics;

- Putting the citizen at the centre of the crisis management process, increasing their capacity to access, read and interpret scientifically sourced information, analysing gender behaviours regarding unpopular measures (e.g., quarantine) and vaccination attitudes and identification and relieving of barriers for vaccination readiness: Trust, risk appraisal, barriers for registration for vaccination, information, collective responsibility;

- Incorporation of information technology and bias-free data processing into crisis management through improved information processing in transformative governance, illustrating possibilities, challenges, and limits of digitalisation and enabling usage of data for political decision making;

- Incorporation of machine learning and artificial intelligence in governance and political decision making based on interdisciplinary discussions on definitions on problems; areas of application; and definition of responsibilities and competences in data governance;

- Validation of novel, smartphone sized or wearable technologies with laboratory-level diagnostics capability (e.g., wearables with integrated digital dosimeters, handheld PCR test devices);

- Strengthening of the One Health approach including not only human physical health but also mental health as well as environmental and animal health, and understanding of the biological risks posed by environmental changes such as climate change and preparedness for impacts on human health;

- Projects should include privacy safeguards to ensure that disaster response systems protect fundamental rights such as privacy and protection of personal data.

Scope: The COVID-19 pandemic illustrated the specific challenges of health emergencies and the necessity to be prepared not only on a material and physical level but also from a social and societal perspective. Challenges during the pandemic included difficulties of working with protective gear such as insecurities and usage mistakes; additional disadvantages for vulnerable groups among others due to communication issues; and lack of local cooperation and prevention regarding equipment, stocks, and coordination. These challenges were largely due to deficiencies in the inclusion of social sciences in disaster research. The COVID-19 pandemic poses an opportunity to analyse successes and difficulties during a global health crisis and thereby preparing for future health crises.

Currently, different groups are not reached equally by public communication efforts. Risk communication especially fails to contact vulnerable groups. Social inequalities are present in different forms and on different levels. For communication strategies and interventions, it should be considered how they are affected by different groups, localities, and cultural factors. In different crises, different vulnerability factors can be more pronounced and different groups can be more vulnerable. On the other hand, resilience can protect against negative effects of crises. Resilience can be supported on an individual, organisational, or systemic level. All should be considered in preparation for crisis as well as in acute situations.

Information technology and digital data processing are becoming increasingly important in public health issues, including personal data protection and ethics. Processing large datasets and automated analyses can open new possibilities in understanding health and illness on a population level and for deriving prevention strategies. However, the implementation of information technology poses several challenges and research on how to effectively use the results in political decision-making. Data security is another challenge when large amounts of personalized (health) data are processed automatically. Concerns about data security and general scepticism about digital information processing in the population need to be taken seriously and addressed.

Health encompasses several aspects and levels. Human health incorporates both physical and psychological health which are interconnected and mutually dependent. At the same time, humans are embedded in their environment so human and environmental health cannot be approached in isolation from each other. According to the One Health approach, health of humans, animals, and environment are intertwined. This is illustrated by the current health crisis of COVID-19 which is attributed to SARS-CoV-2 jumping over from wild animals to humans. Another illustration of the interconnectedness are health impacts of climate change. These interdependencies make an interdisciplinary approach to health necessary that incorporates all aspects of health and their interconnectedness.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH as well as gender experts, institutions as well as the inclusion of relevant SSH and gender expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related research activities. The involvement of citizens, civil society and other societal

stakeholders in co-design and co-creation should be promoted. In order to achieve the expected outcomes, international cooperation is encouraged.

DRS03 - Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-02: Operability and standardisation in response to biological toxin incidents

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.
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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 National standardisation organisations; For all the participants above, 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.

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

- Improved European crisis management in case of an incident with biological toxins through the development of a pan-European task force of security practitioners, taking into consideration existing intersectoral actions on bioterrorism;
- New and existing portable devices, technologies and methods for responders to perform on-site detection of biological toxins are brought to the market;
- Recommendations of effective decontamination measures for personnel, equipment and facilities exposed to biological toxins are provided based on solid experimental testing;

- Development of an operational European response network of specialised and forensic laboratories, taking into account existing initiatives such as e.g. the HERA Laboratory Network and harmonised procedures/guidelines for forensic analysis of biological toxins applicable to a range of relevant technologies and toxins;

- The risks for responders from exposure to biological toxins in the hot-zone are assessed and recommendations of protective equipment for working with biological toxins in the hot-zone are developed;

- Building on existing initiatives and networks, a consolidated platform is established providing support for standardisation efforts in the analysis of biological toxins.

Scope: Recent incidents in Europe and worldwide have highlighted the current threat posed by several biological toxins falling under the Chemical and Biological Weapons Convention. The incidents demonstrated the urgency for countries individually and collectively to improve crisis management capabilities, to advance standardisation efforts and to interconnect security practitioners such as first responders (including health emergency services), law enforcement agencies, specialists from public health (e.g. epidemiologists, environmental health experts), as well as specialised and forensic laboratories across Europe. In order to ensure cross border interoperability, existing and new national procedures need to be developed and implemented in an operational and coherent European crisis response network capable of addressing the threats posed by biological toxins.

To properly manage and minimise the effects of an attack with biological toxins, fast and reliable detection and identification of the used agent is critical. Portable devices, technologies and methods for responders to perform on-site detection of a panel of biological toxins remain to be developed. There is a need for evaluation, training and advancement of on-site detection methods for responders, as well as the integration of emerging detection technologies into marketable solutions.

The safety of responders relies on correct risk assessment and the use of appropriate protective equipment. The risks from exposure to biological toxins in the hot zone are largely unknown. In order to recommend appropriate protective equipment for first responders and to guide the use of effective decontamination measures, the risks from exposure need to be assessed, taking into account sex susceptibility to toxins exposure. The Commission stockpiles personal protective equipment, and links should be sought with this joint DG ECHO-HERA action to make proposals as useful as possible.

Following an attack, exposed personnel, equipment and facilities needs to be decontaminated and declared safe as quickly as possible, in order limit the effects on society. Most decontamination procedures are developed for chemical or biological (i.e. organisms and viruses) agents, but based on their characteristics, biological toxins are at the interface of classical biological and chemical agents. Therefore, the efficiency of existing decontamination procedures should be evaluated for the decontamination of biological toxins.

Previous initiatives have initiated standardisation efforts for lab-based detection and identification of biological toxins. Analytical tools and reference materials are available and comprehensive training and proficiency-testing programs were organised, however, the need for further technical and operational improvement was demonstrated. Building on existing initiatives and networks, a consolidated platform should be established providing analytical tools (including Certified Reference Materials), training and intercomparisons among laboratories. Following the initial detection of the used biological toxin, a more detailed analysis is needed in order to link the agent to confiscated materials. In support of criminal investigations, new procedures and guidelines for comprehensive forensic analysis of biological toxins are needed. The developed methods and procedures should be shared among specialised and forensic laboratories. This action is also expected to engage with the European Health Emergency Preparedness and Response Authority (HERA).

In this context it is important to remind that standardisation should support operations and policymaking to supplement it but should by no means substitute it. While standardisation of technology may be more straightforward, the right balance does especially have to be sought for processes. The action should ensure close synergies with standardisation activities on European (e.g. CEN/TC 391) and international level (e.g. ISO/TC 292).

HORIZON-CL3-2023-DRS-01-03: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors

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	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of: • at least 3 Training Centres located in the European Union; • in addition, the consortium must include at least 2 CBRN Centres of Excellence [70] from targeted non-associated third countries; • and representatives of scientific stakeholders involved in training,

[70] Reference to be added (list of CBRN CoEs)

	validation and testing of CBRN-E tools and technologies and end-users (both practitioners and policymakers). For all the participants above, 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.

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

- Extended networking of training centres in Europe and selected CBRN Centres of Excellence in non-EU countries;
- Compilation of information of capacities of networked CBRN-E training centres in view of better coordination of training and testing actions in support of research and standard developments;
- Improved cooperation and development of testing methodologies and protocols for the validation of tools and technologies resulting from research actions (including pre- or co-normative research) and/or proofs of concepts for developing standards, combining societal and technological challenges;
- Inter-cooperation through an established forum of training centres to synchronize actions for identifying gaps in test and validation techniques, methodologies and protocols.

Scope: In case of a CBRN-E incident, it is of outmost importance that personnel involved in handling the situation, i.e., rescue services and polices, are well educated and trained and that they are using equipment and tools that are reliable with validated capabilities. It can be the difference between a well-functioning management and a disaster. To achieve a more robust and consistent opportunity to practice, test and evaluate CBRN-E tools and technologies (resulting from research actions and/or standard developments) within Europe and beyond, it is necessary to strengthen networking of existing training and testing facilities and centres and to extend it to relevant CBRN Centres of Excellence located in non-EU countries. An assessment of such facilities can identify gaps where training and testing opportunities are lacking but can also be a possibility to highlight weaknesses in that there may be dependencies on one or a few actors. This will indicate what type of facilities are ready to be used for specific training / validation needs and which developments are required to strengthen the testing end exercise capabilities to be better prepared in the event of a CBRN-E incident. It will also give the existing centres a possibility to cooperate to compare, enhance, develop and extend the range of tests, exercises and training to achieve a robustness that will benefit the whole European CBRN-E community. Along validation / testing actions, training exercises should consider societal aspects (vulnerable groups, human factors) in combination of CBRN technological response in case of an incident. It should be considered whether the

Commission stockpiled items, aiming to respond to medical and CBRN emergencies, could be a part of training and validation exercises.

The work would build on the results achieved from past H2020 and ISF actions in this area, focusing on further development of tools, tests and training methods.

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. The involvement of citizens, civil society and other societal stakeholders in co-design and co-creation should be promoted.

In order to achieve the expected outcomes, international cooperation is required, in particular with countries belonging to the CBRN Centres of Excellence network.

DRS04 - Strengthened capacities of first and second responders

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-04: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments

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.
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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and representatives of local or regional authorities in charge of managing hazardous environmental sites from at least 3 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. 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.

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

- Broad acceptance of autonomous systems by first responders and affected people in civil protection;
- Higher safety and security standards for operational forces working in hazardous environments;
- Get ahead of future shortcomings of trained first responder personnel by increasing first responder efficiency (less personnel do more work in shorter time);
- Increased ability to conduct on-scene operations remotely without endangering first responders;
- European robotics industry is strengthened through engagement in the civil protection research as well as an economic and political advantage through building up know-how for innovative technologies;
- Reduction of false positive redouts from various sensors carried by robots.

Scope: Robotics and automation are key technologies that help increase productivity and efficiency to prevent, prepare, and/or respond to natural and human-made disasters. Demographic change and lifestyle changes, such as shifting several time centre of one's life, build up lots of pressure, especially on volunteer-based first responder organizations, which need long training to be mission ready. First responders supported by robotics will be able to fulfil more work within a shorter amount of time and with less personnel. In this industry, cheaper, more capable, and more flexible technologies are accelerating the growth of fully automated production facilities. It is necessary to bring this innovation also into saving lives. Fundamental changes (procedures, tactics and strategies) in the civil protection traditional way of working are needed. Robotic systems with and without autonomous functionalities are not entirely new in disaster relief, but still, there is no continuous and decisive step towards bringing this innovation into the first responders' daily work. In order to be successful in this process, various aspects should be considered.

Firstly, there is a need to identify the fields and domains that will benefit from (autonomous) robotic systems. For a start, there is an urgent need to look into the deployments in hazardous environments or where the danger for first responders and citizens is the highest. What kind of technologies can be replaced with robotic solutions to complete the task more efficiently? What are the situations which cause the most significant danger to human life during a disaster situation? Also, it is essential to look into options where robotic systems might be

more effective than humans. Extensive technology inventory is needed. Altogether this first step can be considered as the exhaustive requirements and gaps analyses which is an inevitable step bringing robotics closer to the civil protection.

Secondly, the identified gaps and needs should be the basis for proof-of-concept research and development studies. Proof of concept studies can either focus on autonomous systems or semi- autonomous systems (e.g. optionally manned or tele-operated systems). These solutions enable managers and practitioners to immerse themselves in what is happening on- site from a great distance and make decisions or even actively intervene in what is happening. To this end, new sensing capabilities should be developed to enhance robotic capabilities and provide more information about the hazards in the environment they operate. They should be adapted in a compact system to be mounted on robots. Human-machine interaction technologies that enable an overlapping control of the robotic systems between the artificial Intelligence entity and the operator need to be developed. The interaction between the user and the robotic system has to be intuitive and should work without extended training. Thirdly, first responders' training, preparedness, and mindset should be considered when bringing new technologies into the field. This is necessary in order to reach a required paradigm shift. This is a long-term process and therefore has to be strategical and well planned.

Fourthly, the relevant infrastructure needs to be put in place. Robotic systems should be seen as an integral part of first responder ecosystems and not as a single technology. Further research is needed to define the basic physical and organisational structures and facilities required for the operation of robotic solutions and integration to the current operational infrastructure. Therefore, adapted standard operational procedures have to be developed.

Overarching topics like ethics, legal and societal implications are highly relevant in the robotics context. They form the basis for the societal acceptance of artificial intelligence in control and decision-making. As robotics become a new resource for the application in hazardous environments (but not only), their acceptance has to be ensured from the perspectives of emergency services, just as the people to be rescued.

In summary, the scope of this topic is not only to develop new robotic solutions for specific tasks but addresses also more holistically the surrounding environment and factors that impact civil protection on a larger scale (urbanisation, ageing, climate change, increased complexity in the area of critical infrastructure protection etc.). There are many research and engineering challenges that need to be addressed in the framework of this topic. First responders play a vital role in ensuring that the robotics solutions are based on the needs and are valuable assets for the civil protection ecosystem.

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/innovation activities.

In order to achieve the expected outcomes, international cooperation is encouraged.

HORIZON-CL3-2023-DRS-01-05: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

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 3.50 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and 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 "Eligibility information about practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. 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).

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

- Identification and evaluation of existing technologies supporting first and second responders in their immediate response to natural disasters (e.g. drones, AI, sensors), highlighting their strengths and weaknesses;
- Testing and implementation of most promising user-centred technologies in real-world conditions;
- Innovative technology solutions to improve searching operations in smoky environments in the case of wildfires.

Scope: Supplying relief items to various demand spots in disaster-prone areas is a critical task due to last-kilometer logistics problems that hamper the process of and efficient transportation

of first responders and their equipment. Blocked roads, heavy terrain and bad weather conditions are factors that are faced by first and second responders (e.g. fire brigade, emergency medical services) in the immediate response to disasters. Innovative technologies (e.g. drones, AI, sensors etc.) are considered to support emergency workers in overcoming the aforementioned challenges related to relief items delivery and can provide ability to obtain critical information remotely about the extent, perimeter, or interior of the incident as well as conduct on-scene operations remotely without endangering responders. For example, technology solutions for navigation in smoky environments in the case of wildfires can potentially increase the efficiency of search operations by fire fighters.

Call - Disaster-Resilient Society 2024

HORIZON-CL3-2024-DRS-01

Conditions for the Call

Indicative budget(s)[71]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[72]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-DRS-01-01	RIA	8.00	Around 4.00	2
HORIZON-CL3-2024-DRS-01-02	IA	6.00	Around 3.00	2
HORIZON-CL3-2024-DRS-01-03	RIA	4.00	Around 4.00	1
HORIZON-CL3-2024-DRS-01-04	RIA	6.00	Around 6.00	1
Overall indicative budget		24.00		

[71] 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 years 2023 and 2024.

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

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.

DRS02 - Improved Disaster Risk Management and Governance

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-01: Prevention, detection, response and mitigation of chemical, biological and radiological threats to agricultural production, feed and food processing, distribution and consumption

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3

	organisations representing citizens or local communities, practitioners (first and/or second responders), and local or regional authorities and private sector from at least 3 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. 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).
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Increasing EU capabilities to assess risks, detect, alert, mitigate and respond to feed and food intentional and accidental contamination from chemical, biological and radiological (CBR) agents, through the entire food chains (soils and agro-production, feed and food industry, transporting, retail and hospitality industry, public catering);
- Increasing the understanding on food terrorism threats and on food chain vulnerabilities to intentional and accidental contaminations;
- Raising awareness among feed and food companies and authorities to CBR threats arising from malicious use of hazardous agents that pose danger to animal and public health. This should be done under the premises of feed and food as a critical infrastructure and risks pertaining therein;
- In addition to raising awareness, proposals should develop possible preparedness, mitigation and response plans for national authorities and the private sector.

Scope: Plant and animal health is of global importance for sustainable agriculture and competitive agriculture and forestry, as well as for the protection of biodiversity and ecosystems[73]. Globally, between 10 and 28 percent of crop production is lost to pests and contamination of food and feed by mycotoxins can severely threaten the health of humans and livestock. The International Year of Plant Health (IYPH) 2020, established by the United Nations, raised public and political awareness of the importance of plant health and a recent study (IPPC, 2021) calls the attention of policy makers to the main effects of climate change

[73] For R&I on plant and animal health as well as on agro-biodiversity please consult further topics under the Cluster 6 Work Programme.

on plant health, helping governments and the international community addressing plant health challenges. Also, the food chain, from harvest of agricultural products, throughout processing, distribution and until consumption can be challenged by several (hybrid) threats, which are increasingly taking non-conventional forms and possibly targeting the agriculture and food chain with severe consequences.

The Word Health Organisation identified intentional agriculture attack with biological weapons and food contamination as one of the main global public health threats of the 21st century. The potential for terrorist attacks or other criminal actions against agri-food targets is increasingly recognised as a threat to international security. The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by CBR agents. These risks have been studied and documented by a Network of excellence (Plant and Food Biosecurity) funded by the European Commission under the 7th Framework Programme (PLANTFOODSEC).

In 2017, the ENVI Committee (Committee on Environment, Public Health and Food Safety of the EU Parliament) has defined food defence as *"the protection of food from intentional contamination or adulteration by biological, chemical, physical or radiological agents. It includes measures regarding prevention, protection, mitigation, response and recovery form intentional acts of food contamination".* The potential impact on human health of deliberate sabotage of agricultural crops, seed or food can be estimated by extrapolation from the many documented examples of unintentional outbreaks of foodborne disease.

Current EU capabilities to detect and respond to agro-terrorism and bio-criminal acts are dispersed across different national practitioners, normally handled by regional or national bodies and are very limited in terms of coordination. Different countries have different governmental authorities for agricultural and feed and food domains, different collaborative networks, different border controls, different inspection bodies and different regulatory references and reporting mechanisms as well as different investigative bodies in the case of suspected feed/food crime. The EU institutions have to start to consider the agri-food chain as a critical infrastructure which can suffer from attacks and which need to be protected. The most effective way to accomplish this goal is through international cooperation by a multi-sectorial approach combing different expertise, such as from law enforcement, the feed and food sector and health emergency services.

The main challenge is to increase the resilience of European agricultural production, feed and food processing and distribution chain in case of sudden shocks. Agriculture and food chains will be included as an important dimension to be analysed in the context of protection of European critical entities [74] in case of emergencies. It is also crucial to address the interrelations between the food chain shocks and different types of critical entities with the objective of developing tools and methods to minimize cascading effects and allow rapid recovery of service performance levels after incidents. In the new context also the interaction with climate change, global trade and internet trade (spreading often plant material not

[74] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities (COM(2020) 829 final.

controlled at all and of low quality) need to be taken into consideration. Artificial intelligence provides new tools for better coping with many of the most important challenges.

In this context, research should address agri-food systems shocks, taking account of the increasing effects of climate change and global trade (and their interaction) on pest outbreaks and spread, feed/food commodity shocks, due to external challenges, feed/food supply chains interruption and organised agri-food terrorism attacks.

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.

In order to achieve the expected outcomes, international cooperation is also encouraged.

Coordination among the successful proposals from this topic as well as with the successful proposal(s) under topic *HORIZON-MISS-2023-SOIL-01-02: Soil pollution processes – modelling and inclusion in advanced digital decision-support tools* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

DRS03 - Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-02: Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least

	one organisation representing each of the following: - Practitioners (first and/or second responders), - Local and/or regional authorities, - Standardisation organisations, from at least 3 different EU Member States or Associated countries. For all the participants above, 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.

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

- Enhanced links between scientific community and first and second responders promoting user-targeted research and faster transfer of science results into best practices;
- Enhanced adoption of novel technologies such as advanced Earth Observation capabilities and capabilities such as those from Earth Observation space technologies into prevention and management practices and tools;
- Improvement of meteorological input (wind, temperature, precipitation, soil humidity) for extremes related to heat and drought (forest fires, heatwave, agricultural damage, low water for hydro power), especially concerning the support of counter activities;
- Improved methods for cross-border and cross-sectoral knowledge transfer about risk, vulnerability, exposure, and monitoring methods;
- Development of common technical standards of alert and impact forecasting systems that cope more efficiently with transboundary emergencies and for GIS-based information systems dealing with high-impact weather / climatic and geological disasters management during emergencies;
- Identification of needs and opportunities for transferring advanced scientific results into enhancement in disaster logistics and responses, including tailor-made education and training programmes for emergency management teams.

Scope: Europe is confronted with increasingly intense and sometimes unexpected consequences of natural disasters ranging from floods and heavy rain events to droughts and large-scale forest fires even in hitherto not affected regions, as well as other geohazards such as volcanic eruptions and landslides. To respond to these emerging challenges an integrated transnational emergency management is needed efficiently linking systems available at the European level such as, for example, the Copernicus Emergency Management Service, with

national, regional or local systems. Furthermore, an evaluation of applied disaster risk reduction methods is required, in particular alert and impact forecasting systems, to identify potential for improvement and constant innovation.

Knowledge transfer (cross-border and cross-sectoral) about natural hazards-related risks and emergency management is essential to increase the resilience of societies. A vital dialogue and exchange of good practice examples among scientific and technical communities, stakeholders, policymakers and local communities is needed. In particular, the level of awareness of EU citizens for local risks can be increased by new approaches to visualise risks, vulnerability and exposure through e.g. impact forecasting data and mapping including satellite data and information. Emergency management plays a crucial role in this regard, taking into account the ongoing urbanization and economic growth, which put a lot of pressure on areas such as floodplains and their ability to absorb and store water.

Currently, there are no harmonised / standardised European methods for identifying vulnerability and exposure on the basis of which alert and impact forecasting systems are established, allowing this information to be used by civil protection authorities in a timely manner to improve disaster preparedness, communication to local authorities and population, evaluation logistics etc. Recent flash floods in Belgium, Germany and Luxembourg in July 2021 have shown that this lack of protocols hampered the efficient implementation of early warning and preparedness actions prior to the disaster event.

This topic is part of a coordination initiative between ESA and the EC on Earth System Science. Under the EC-ESA Earth System Science Initiative both institutions aim at coordinating efforts to support complementary collaborative projects, funded on the EC side through Horizon Europe and on the ESA side through the ESA FutureEO programme. Proposals should include a work package, means and resources for coordination with complementary projects funded under the Science for Society element of the ESA FutureEO programme. The projects(s) should establish a close coordination and collaboration with the relevant ESA relevant actions and projects (https://eo4society.esa.int).

In this context it is important to remind that standardisation should support operations and policymaking to supplement it but should by no means substitute it. While standardisation of technology may be more straightforward, the right balance does especially have to be sought for processes. The action should ensure close synergies with standardisation activities on European and international level.

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/innovation activities.

In order to achieve the expected outcomes, international cooperation is also encouraged.

DRS04 - Strengthened capacities of first and second responders

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-03: Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster

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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and representatives of local or regional authorities in charge of managing NaTech events from at least 3 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. 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.

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

- Development of a holistic vision of crisis management after telluric (e.g. volcanic, seismic, tsunami, landslide) or extreme climate events (e.g. floods, storms, storm surges, fires, droughts) producing impacts on critical assets (e.g. infrastructures, industries) and creation of new management framework for handling NaTech crises;

- Enhanced existing crisis management tools to develop a common platform (shared among public and private operators) allowing cross-border exchanges and decision-making, while respecting legal frameworks and responsibilities;

- Demonstrated operational protocols and development of standard operating procedures able to respond to NaTech crises in cross-border configurations, including comprehensive risk modelling of worst-case scenarios taking into account cascading effects and future impacts of climate change, and taking into consideration spatial information and data;

- Improvement of our understanding and capabilities to identify and mitigate risks associated with interdependencies across infrastructures and other human (social and economic) systems.

Scope: The confluence of incidents in recent years has brought renewed concerns over our systemic resilience to external shocks arising from natural-technological (NaTech) disasters. This is particularly acute in the event of disruption in the transport, power, water supply and communication sectors in highly populated and industrialised areas, or when such events raise the likelihood of cascading effects with severe impacts on communities and the economy that are hard or impossible to predict. The main focus on NaTech risks lies on a thorough understanding of the vulnerability of industrial sites and critical infrastructure, and the potential impact natural hazards can have on such technological resources. This entails the identification of both physical (safety of building facilities and structures) and operational vulnerabilities, often addressing multi-hazard conditions. Innovative methods are required for analysing worst-case scenarios, and informing decision-makers about the crosscutting and shared responses to different crises given available resources.

Research involving multiple fields of expertise, including spatial information (to be specified), is also required to improve hi-tech capacities for operational response systems to better cope with natural and/or technological disasters occurring in Europe (and in overseas territories) in an integrated manner. This will rely on a knowledge sharing among natural and technological risks communities to develop a holistic vision for an integrated operational crisis management of NaTech disasters.

This topic is part of a coordination initiative between ESA and the EC on Earth System Science. Under the EC-ESA Earth System Science Initiative both institutions aim at coordinating efforts to support complementary collaborative projects, funded on the EC side through Horizon Europe and on the ESA side through the ESA FutureEO programme. Proposals should include a work package, means and resources for coordination with complementary projects funded under the ESA FutureEO initiative.

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/innovation activities.

In order to achieve the expected outcomes, international cooperation is encouraged. The action should take due consideration to EU policies, in particular the SevesoIII and CER Directives, and ensure close synergies with international conventions such as the Convention on the Transboundary Effects of Industrial Accidents (TEIA) / Implementation of natural hazard-triggered technological accident principles, and the Sendai Framework for Action.

HORIZON-CL3-2024-DRS-01-04: Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident

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.
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: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and representatives of local or regional authorities in charge of managing Nuclear Installations from at least 3 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. 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.
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: Projects' results are expected to contribute to some or all of the following outcomes:

- Based on existing national practices, improved understanding of the radioactive fallout and methodology regarding robust and rapid monitoring of dose rate and nuclide specific determination with purpose of facilitating safe evacuation after a nuclear or radiological event;
- Improved tools and methods for risk assessment following a nuclear or radiological event and optimized actions after a disaster that are based on risk analysis rather than probabilities
- Identification of the relevant range of different protective measures, including medical countermeasures, needed after a RN disaster, and improved protection of population and infrastructures through better analysis of sensor data resulting in adequate protective actions;
- Improved understanding of contamination and decontamination of population and infrastructure, and improved rapid procedures for decontamination of individuals after a RN-incident;
- Recommendations on integration of improved technologies and assessment methodologies in the RN crisis managements systems.

Scope: A nuclear explosion in any EU member country (or in the European neighbourhood) would lead to disastrous effects for numerous EU citizens and residents. For example, the initial effects from a nuclear explosion in a city will lead to, besides numerous dead and severely injured citizens, destroyed infrastructure. The radioactive plume containing particulate matter may damage ventilation systems and fallout will generate high dose rates. Criticality or other incidents at nuclear power plants and nuclear-powered vessels may occur because of direct attack, sabotage, collateral damage, accidents, loss of infrastructure services such as power and/or water supply or lack of necessary skilled personnel on site.

Research on large-scale protection of population and infrastructure in the event of a nuclear explosion need to be undertaken both separately as well as in a RN-perspective. Research activities aimed at updating EU's possibilities for large-scale protection of population and infrastructure in the event of a nuclear explosion would benefit from being carried out in close cooperation with other EU-members. Research activities should also pertain to improved understanding of the radioactive fallout and assessment of dose rates to the population following a nuclear explosion in order to enable use of cost-effective sustainable technologies in protection of population and infrastructures.

In a situation after a RN-incident the time consuming and laborious decontamination procedures for the population must be reduced to a minimum. Therefore, the possibility to identifying the need for decontamination, and above all to assess that there is no need for

decontamination would be beneficial as well as the possibility to enter a shelter or other protected area in a safe way.

Protective measures in the aftermath of a RN disaster may vary depending on situations. Such measures should be based on evaluated risks rather than probabilities. Starting with sensor- as well as other available data, measures could be optimized from a risk-cost point-of-view resulting in cost-effectiveness.

Based on measurement data, appropriate protective actions could be decided upon. If a risk analysis results in a low risk, a lower level of mitigating measures might be needed resulting in lower costs. Then resources can be used in other areas where they are more needed, leading to an overall optimized protection.

Protective actions should be based on risk modelling. Such modelling is based on available knowledge of different input quantities resulting in a probability distribution, from which the risk can be calculated applying a consequence function.

New technologies should be compatible with RN crisis management systems, strategies for crisis communication and take into account relevant societal and human factors, such as vulnerable group and cultural and linguistic diversities. In order to achieve the expected outcomes, international cooperation is encouraged. The action should take due consideration to EU policies, in particular the SevesoIII and CER Directives.

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/innovation activities.

Within this topic, the European Commission encourages all potential participants to create, where possible, opportunities for the affected persons and entities, in particular researchers and innovators previously active in Ukraine as well as Ukrainian researchers and innovators who are unable to return to Ukraine in the given circumstances.

Destination - Strengthened Security Research and Innovation

The EU-funded security research and innovation framework was launched with the Preparatory Action for Security Research[75]. Since then, the programme has contributed substantially to knowledge and value creation in the field of internal security and to the consolidation of an ecosystem better equipped to capitalise on research and innovation to support the EU security priorities.

While the success of the programme has materialised in relevant scientific findings, maturation of promising technology areas, operational validation of innovative concepts or support to policy implementation, a key challenge remains in improving the uptake of innovation.

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, thus contributing to the development of security capabilities[76], could give a valuable measure of the impact achieved with the programme. However, as explained in the Commission staff working document on Enhancing security through research and innovation[77], there are factors inherent to the EU security ecosystem (often attributed to the market) that hinder the full achievement of this impact. These include market fragmentation, cultural barriers, analytical weaknesses, programming weaknesses, ethical, legal and societal considerations or lack of synergies between funding instruments, among others.

It is worth noting that such factors affect all the security domains addressed in Cluster 3; that there is not one predominant factor with sufficient leverage by itself to change the overall innovation uptake dynamics; and that they exhibit complex relationships among them which are difficult to disentangle. It should also be noted that the innovation uptake process starts before the R&I cycle is triggered, and it is not finalised with the successful termination of a research project. Therefore, the uptake challenge extends beyond the realm of R&I. However, from within R&I it is possible, if not to materialise the uptake in every case, at least to pave the way towards its materialisation.

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, that is visible and recognisable to those interested in contributing to this aim, and which provides bespoke tools that serve to tackle the factors that hinder innovation uptake.

---

75 COM(2004) 72.

76 For the purpose of this 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.

77 SWD(2021) 422.

The SSRI Destination has therefore been designed with this purpose to serve equally to all the expected impacts of Cluster 3. Research applied in this domain will contribute to increasing the impact of the work carried out in the EU security Research and Innovation ecosystem as a whole and to contribute to its core values, namely: i) Ensuring that security R&I maintains the focus on the potential final use of its outcomes; ii) Contributing to a forward-looking planning of EU security capabilities; iii) Ensuring the development of security technologies that are socially acceptable; iv) Paving the way to the industrialisation, commercialisation, acquisition and deployment of successful R&I outcomes; and v) Safeguarding the open strategic autonomy and technological sovereignty of the EU in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base.

While the other Destinations of this Horizon Europe Cluster 3 Work Programme offer research and innovation activities to develop solutions to address specific security threats or capability needs, the SSRI 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 described in the Commission staff working document on security research. 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.

In addition, the SSRI Destination will offer an open environment to create 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. This will contribute to reducing thematic fragmentation, bringing closer together the actors from different security domains, and expanding the market beyond traditional thematic silos.

Finally, SSRI will allow the allocation of resources to the development of tools and methods to reinforce the innovation cycle itself from a process standpoint, thus increasing its effectiveness, efficiency and impact. This Destination will contribute to the development of the tailored analytical capacity required for the adoption of capability-driven approaches, in line with the provisions of the Action Plan on synergies between civil, defence and aerospace industries[78] and with the measures set out in the Commission staff working document on security research aimed at fostering a forward-looking capability-driven approach in security.

In order to accomplish the objectives of this Destination, additional eligibility conditions have been defined with regard to the active involvement of relevant security practitioners or end-users.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following impacts:

[78] COM(2021) 70.

- 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.

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) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-SSRI-01	6.50		23 Nov 2023
HORIZON-CL3-2024-SSRI-01		14.00	20 Nov 2024
Overall indicative budget	6.50	14.00	

Call - Support to Security Research and Innovation 2023

HORIZON-CL3-2023-SSRI-01

Conditions for the Call

Indicative budget(s)[79]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[80]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-SSRI-01-01	CSA	2.00	Around 1.00	2
HORIZON-CL3-2023-SSRI-01-02	IA	4.50	Around 1.50	3
Overall indicative budget		6.50		

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.

79 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 years 2023 and 2024.

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

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.

SSRI 02 - Increased innovation uptake

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-SSRI-01-01: Open grounds for pre-commercial procurement of innovative security technologies

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: The following additional eligibility conditions apply: This topic requires the participation of at least 6 relevant end-user organisations as well as at least 3 public procurers from at least 3 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. One organisation can have the role of end-user and public procurer simultaneously, both counting for the overall number of organisations required for eligibility. Open market consultations carried out during this project must take place in at least three EU Member States or Associated Countries.
Legal and financial set-up of	The rules are described in General Annex G. The following exceptions

the Grant Agreements	apply: 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). [81].

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

- Consolidated demand for innovative security technologies built on the aggregation of public buyers with a common need expressed in functional and/or operational terms without prescribing technical solutions;
- Better informed decision-making related to investment in innovative security technologies based on a better understanding of the potential EU-based supply of technical alternatives that could address common needs of EU public buyers;
- Better informed decision-making related to investment in innovative security technologies based on an improved visibility of the potential demand in the EU market for common security technologies;
- 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;
- Increased innovation capacity of EU public procurers through the availability of innovative tendering guidance, commonly agreed validation strategies and evidence-based prospects of further joint procurement of common security solutions.

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 action. Both this preparatory action and the future PCP action are open to proposals oriented to the acquisition of R&D services for the development of innovative technologies, systems, tools or techniques to enhance border security, to fight against crime and terrorism, to protect infrastructure and public spaces, and/or to make societies more resilient against natural or human-made disasters.

The project funded under this topic should also consider submitting a proposal to an open call for a follow-up PCP action that the Commission may include in the Cluster 3 Work

[81] 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

Programme 2025-2027 (subject to budget availability and priorities of the Work Programme 2025-2027). In preparing the grounds for a possible future PCP action, the outputs of this CSA should take into consideration:

- 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 aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) can be 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.

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

The project should have a maximum estimated duration of 1 year.

HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

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: Consortia must include: - A minimum of three (3) to a maximum of seven (7) partners. - At least 2 SMEs from 2 different Member States. - At least 1 end-user organisation relevant per area. - At least 3 Member States or Associated Countries must be represented in the consortium. Participation of non-SME industries and RTOs is not excluded, but it must be limited to 15% of the budget. At least 50% of the budget must be allocated to SMEs.

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: To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the four options • Option A ''Fighting Organised Crime and Terrorism'' • Option B ''Disaster Resilience'' • Option C ''Resilient Infrastructure'' and • Option D ''Border Security'', 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: 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). [82].

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

- Development of a mature technological solution addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme.
- Facilitated access to civil security market for small and medium innovators and enhanced links between suppliers and public buyers;
- Improved cooperation between public buyers and small supply market actors for a swifter uptake of innovation in response to short to mid-term needs;
- Stronger partnerships between small and medium EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and increase technological sovereignty of the EU in critical security areas.

[82] 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: 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 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.

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.
- Not overlapping with the scope of the topics included in the other destinations of this 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.

The involvement of big industries in the projects should not focus on technology development but on supporting the SMEs in bringing their innovations to the market. Examples of activities include but are not limited to, acting as first buyer/integrator of the developed technologies, 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. In the same fashion, the participation of research and technology organisations should not focus on 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. Exceptions to this requirement should be duly justified.

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

In this call, projects should address the areas of Border Management, INFRA, Disaster Resilience, Fighting Crime and Terrorism. Some examples of domains that could be addressed under the BM area are (indicative and non-exhaustive): facilitated border checks; secure documents and identity management for border crossings; border surveillance; detection of drugs, explosives, 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. Some examples of domains that could be addressed under the INFRA area are: (indicative and non-exhaustive): physical access control, autonomous systems used for infrastructure protection, positioning and localisation tracking and tracing, monitoring and surveillance of environments and activities. Some examples of domains that could be addressed under the DRS area are (indicative and non-exhaustive): data and satellite/remote sensing information exploitation, positioning and localisation tracking and tracing, monitoring and surveillance for disaster prevention. Some examples of domains that could be addressed under the FCT area are: (indicative and non-exhaustive): mobile forensics; deepfake detection; detection of counterfeiting (fake items, fake currency bills) or of 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.

Only one project per area will be funded, with the total number of funded projects being three. The area excluded will be the one whose project proposal receives the lowest marking compared to the other three areas.

In this call, projects should address the EU security policy priorities in the areas addressed by the Cluster 3 work programme.

In this topic, the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement.

Call - Support to Security Research and Innovation 2024

HORIZON-CL3-2024-SSRI-01

Conditions for the Call

Indicative budget(s)[83]

[83] 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.

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[84]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-SSRI-01-01	PCP	6.00	Around 6.00	1
HORIZON-CL3-2024-SSRI-01-02	IA	8.00	Around 2.00	4
Overall indicative budget		14.00		

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.

SSRI 02 – Increased innovation uptake

Proposals are invited against the following topic(s):

[84] The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.
Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

HORIZON-CL3-2024-SSRI-01-01: Demand-led innovation through public procurement

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.
Indicative budget	The total indicative budget for the topic is EUR 6.00 million.
Type of Action	Pre-commercial Procurement
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility conditions apply: This topic requires the participation of at least 3 relevant end-user organisations and 3 public procurers from 3 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. One organisation can have the role of end-user and public procurer simultaneously, both counting for the overall number of organisations required for eligibility.
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: PCP/PPI procurement costs are eligible. The specific conditions for actions with PCP/PPI procurements in section H of the General Annexes apply to grants funded under this topic. Beneficiaries must ensure that the subcontracted work is performed in at least 3 Member States — unless otherwise approved by the granting authority.

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

- An identifiable community of EU civil security authorities with common user/functional needs for innovative technology solutions;

- Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes that meet the needs of the EU user community;

- 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: End-users and public procurers from several countries are invited to send proposals for launching a Pre-Commercial Procurement action for the acquisition of R&D services for the development of innovative civil security technology solutions.

The proposals should build on the outcomes of CSA projects funded under previous work programmes aimed at creating *Stronger grounds for pre-commercial procurement of innovative security technologies [for example, topic HORIZON-CL3-2022-SSRI-01-03: Stronger grounds for pre-commercial procurement of innovative security technologies.]*. The successful proposals could therefore give continuity to the works initiated by those CSA projects.

The proposals are expected to provide clear evidence on a number of aspects in order to justify and de-risk the 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 end-users and procurers 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 to the needs, and that there are different technical alternatives to address the proposed challenge;

- That the PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready in due time in order to launch the call for R&D services according to the PCP rules.

- That there is a commitment to pursue the exploitation of results beyond the end of the project through engagement with stakeholders and implementation of exploitation strategies towards future uptake.

The open market consultations required prior to launching the PCP call for tenders must have taken place in at least three EU Member States. Market consultations conducted during the previous CSA projects can be used if this requirement is fulfilled, and if it is justified that: i) their purpose was enough to guarantee the viability of the procurement and; ii) that the state-of-the-art has not changed since they were conducted.

In relation with the PCP tendering process, the applicants should clarify how they intend to guarantee that:

- The principles of the EU Directive for public procurement and in particular with the provisions related to PCP will be duly respected;
- Conflict of interests will be avoided, including through the ineligibility of bids from technology providers who are also beneficiaries of the project or who have been beneficiaries of the previous CSA projects;
- The confidentiality of the intellectual property of potential bidders will be protected;
- The technology developments to be conducted in the PCP will 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;
- In developing technology solutions, societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) will be taken into account in a comprehensive and thorough manner;
- All participating public buyers commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default;
- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, will be duly taken into account, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

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 resulting from the previous CSA projects, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.
- 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.

The 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.

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

HORIZON-CL3-2024-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

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 8.00 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: Consortia must include: - A minimum of three (3) to a maximum of seven (7) partners.

	- At least 2 SMEs from 2 different Member States. - At least 1 end-user organisation relevant per area. - At least 3 Member States or Associated Countries must be represented in the consortium. Participation of non-SME industries and RTOs is not excluded, but it must be limited to 15% of the budget. At least 50% of the budget must be allocated to SMEs.
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Procedure	The procedure is described in General Annex F. The following exceptions apply: To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the four options: • Option A ''Fighting Organised Crime and Terrorism'' • Option B ''Disaster Resilience'' • Option C ''Resilient Infrastructure'' and • Option D ''Border Security'', 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: 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). [85].

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

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

[85] 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

- Facilitated access to civil security market for small innovators;
- Improved cooperation between public buyers and small supply market actors for a swifter uptake of innovation in response to short to mid-term needs;
- Stronger partnerships between small and medium EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and reduce technological dependencies from non-EU suppliers in critical security areas.

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 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.

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.
- Not overlapping with the scope of the topics included in the other destinations of this 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[86]. Exceptions to this requirement should be duly justified.

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

In this call, projects should address the areas of Border Management, INFRA, Disaster Resilience, Fighting Crime and Terrorism. Some examples of domains that could be addressed under the BM area are (indicative and non-exhaustive): facilitated border checks; secure documents and identity management for border crossings; border surveillance; detection of drugs, explosives, 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. Some examples of domains that could be addressed under the INFRA area are: (indicative and non-exhaustive): physical access control, autonomous systems used for infrastructure protection, positioning and localisation tracking and tracing, monitoring and surveillance of environments and activities. Some examples of domains that could be addressed under the DRS area are (indicative and non-exhaustive): data and satellite/remote sensing information exploitation, positioning and localisation tracking and tracing, monitoring and surveillance for disaster prevention. Some examples of domains that could be addressed under the FCT area are (indicative and non-exhaustive): mobile forensics; deepfake detection; detection of counterfeiting (fake items, fake currency bills) or of 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. Only one project per area will be funded. Priority will be given to the area that did not qualify in the previous call.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement.

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

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.

Form of Funding: Other budget implementation instruments

Type of Action: Expert contract action

Indicative budget: EUR 0.82 million from the 2023 budget and EUR 0.82 million from the 2024 budget

2. Workshops, conferences, experts, communication activities, studies

- Organisation of the Security Research event 2023;
- 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.

Form of Funding: Procurement

Type of Action: Public procurement

Indicative budget: EUR 1.86 million from the 2023 budget and EUR 1.87 million from the 2024 budget

Budget[87]

	Budget line(s)	2023 Budget (EUR million)	2024 Budget (EUR million)
Calls			
HORIZON-CL3-2023-FCT-01		36.00	
	from 01.020230	*36.00*	
HORIZON-CL3-2024-FCT-01			33.70
	from 01.020230		*33.70*
HORIZON-CL3-2023-BM-01		23.90	
	from 01.020230	*23.90*	
HORIZON-CL3-2024-BM-01			24.00
	from 01.020230		*24.00*
HORIZON-CL3-2023-INFRA-01		14.40	
	from 01.020230	*14.40*	
HORIZON-CL3-2024-INFRA-01			12.20
	from 01.020230		*12.20*
HORIZON-CL3-2023-CS-01		50.70	
	from 01.020230	*50.70*	
HORIZON-CL3-2024-CS-01			50.90
	from		*50.90*

87 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 years 2023 and 2024.

	01.020230		
HORIZON-CL3-2023-DRS-01		27.50	
	from 01.020230	*27.50*	
HORIZON-CL3-2024-DRS-01			24.00
	from 01.020230		*24.00*
HORIZON-CL3-2023-SSRI-01		6.50	
	from 01.020230	*6.50*	
HORIZON-CL3-2024-SSRI-01			14.00
	from 01.020230		*14.00*
Contribution from this part to call HORIZON-MISS-2023-OCEAN-SOIL-01 under Part 12 of the work programme		0.32	
	from 01.020230	*0.32*	
Contribution from this part to call HORIZON-MISS-2023-CLIMA-OCEAN-SOIL-01 under Part 12 of the work programme		0.31	
	from 01.020230	*0.31*	
Contribution from this part to call HORIZON-MISS-2023-OCEAN-01 under Part 12 of the work programme		2.05	
	from 01.020230	*2.05*	
Contribution from this part to call HORIZON-MISS-2023-CIT-02 under Part 12 of the work programme		0.11	
	from 01.020230	*0.11*	
Contribution from this part to call HORIZON-MISS-2023-CIT-01 under Part 12 of the work programme		0.90	
	from 01.020230	*0.90*	
Contribution from this part to call HORIZON-MISS-2023-CLIMA-01 under Part 12 of the work programme		1.81	
	from	*1.81*	

	01.020230		
Contribution from this part to call HORIZON-MISS-2023-CLIMA-CITIES-01 under Part 12 of the work programme		0.88	
	from 01.020230	*0.88*	
Contribution from this part to call HORIZON-MISS-2023-SOIL-01 under Part 12 of the work programme		2.09	
	from 01.020230	*2.09*	
Other actions			
Expert contract action		0.82	0.82
	from 01.020230	*0.82*	*0.82*
Public procurement		1.86	1.87
	from 01.020230	*1.86*	*1.87*
Contribution from this part to Specific grant agreement under Part 12 of the work programme		0.95	
	from 01.020230	*0.95*	
Contribution from this part to Expert contract action under Part 12 of the work programme		0.02	
	from 01.020230	*0.02*	
Contribution from this part to Indirectly managed action under Part 12 of the work programme		0.28	
	from 01.020230	*0.28*	
Estimated total budget		171.40	161.49