European Commission

Resilient Infrastructure

CLUSTER 3 – Info day 2025

11 June 2025

Sebastian SERWIAK
European Commission - DG HOME
Innovation and Security Research

Research and Innovation

Destination
“Resilient Infrastructure”

CALL

RESILIENT INFRASTRUCTURE (INFRA)

2025

European Commission

Resilient Infrastructure (INFRA)

RESILIENT INFRASTR.

As stated in the Horizon Europe strategic plan 2025-2027, proposals submitted under this Destination should aim to contribute to:

“[…] resilience of large-scale interconnected systems’ infrastructures and the bodies that operate them in case of complex attacks, pandemics, natural and human-made disasters, or the impacts of climate change[…]”

Specific Impacts include:

- address both physical and digital aspects of critical infrastructure security, including specific challenges for cybersecurity, and
- support development of upgraded systems, and the interoperability of existing systems, for operators’ resilience and the protection of critical infrastructure to enable a rapid, effective, safe and secure response and recovery, as also situational awareness and information sharing, without significant human involvement, to complex threats and challenges while also supporting emergency responders where their intervention is needed;
- security by design is a default feature of both newly created and upgraded infrastructures;
- improve cross-sectoral cooperation, as well as risk assessments to ensure the resilience and open strategic autonomy of European infrastructures.

Resilient Infrastructure – Policy Context

This destination will support the European Commission efforts towards:

- Improving cyber capabilities, coordinating national cyber efforts and securing our critical infrastructures.
- The development of a new European Critical Communication System.
- Building climate resilience and preparedness of infrastructure in sectors like energy, water or food, and informing the new European Water Resilience Strategy.

Moreover:

- Plans to build on elements of relevant predecessor projects should be considered, where relevant. It will be important also to take into account how research results can be advanced to deployable solutions after the projects lifetime, utilising validation and capacity-building programmes like the Internal Security Fund, or Digital Europe Programme.
- 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.

Overview

Code	Topic	mEUR	mEUR per grant	Type of Action
2025-INFRA-01-01	**Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures**	15	5	IA 6-7
2025-INFRA-01-02	**Open topic for role of the human factor for the resilience of critical infrastructures**	7	3.5	RIA 5

Destination
“Resilient Infrastructure” (INFRA)

TOPICS CALL 2025

HORIZON-CL3-2025-INFRA-01-01:

Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures

Expected outcomes:

- Critical infrastructure is more resilient to natural hazards, intentional and accidental harmful human actions, including cyberattacks;
- Critical infrastructure operators and authorities have better mapping of the interdependencies relevant for the addressed sector(s) also in view of better managing potential multi-hazard, cross-sectorial and cross border crisis;
- Critical infrastructure operators and authorities have access to improved monitoring, risk and threat assessment, forecast, and if applicable modelling tools as well as cyber- and physical security solutions;
- Critical infrastructure operators and authorities have access to increased post-incident investigation capabilities contributing to better crisis prevention, preparedness, management and response;
- Effective digital tools to conduct virtual and physical stress tests are available for relevant security practitioners;
- Training curricula for critical infrastructure operators, authorities and/or first responders are developed.

HORIZON-CL3-2025-INFRA-01-02:

Open topic for role of the human factor for the resilience of critical infrastructures

Expected outcomes:

- Critical infrastructure is more resilient to natural hazards, intentional and accidental harmful human actions, including cyber attacks;
- Infrastructure operators and authorities have better understanding of human factor for the critical entities resilience;
- Infrastructure operators and authorities have access to improved risk and threat assessment, and forecast;
- Infrastructure operators and authorities have access to increased post-incident investigation capabilities contributing to better crisis prevention;
- Insider threats are effectively tackled, including through innovative, cost-efficient systems for background checks that are in full compliance with privacy;
- Training curricula for infrastructure operators, authorities and/or first responders are developed.

More Information and resources

ProtectEU: a European Internal Security Strategy

Community for European Research and Innovation for Security (CERIS)

Security Research Event

National Contact points for EU security research

@EUHomeAffairs
#EUSecurityResearch #SecureSocieties

EUHomeAffairs

EU security research: 20 years of innovation, impact, and success

Enhancing security through R&I
CSWD(2021)422

Frontex on EU research

Eu-LISA on EU research

EU Innovation Hub for Internal Security

Horizon Europe Cluster 3 "Civil Security for Society" (2025 published Work Programme)
&
Cluster 3 Info Day and brokerage event 2025

EU Funding & Tenders Portal

European Commission

European
Commission

Thank you!

# HorizonEU

http://ec.europa.eu/horizon-europe

#EUsecurityResearch

Cluster 3

cc BY

© European Union 2021

Unless otherwise noted the reuse of this presentation is authorised under the CC BY 4.0 license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Image credits: © ivector #235536634, #249868181, #251163013, #266009682, #273480523, #362422833, #241215668, #244690530, #245719946, #251163053, #252508849, 2020. Source: Stock.Adobe.com. Icons © Flaticon – all rights reserved.