

Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity

Horizon Europe

● PENDING

Code
HORIZON-CL3-2027-01-INFRA-02

Location
Europe

Scope
International

Curator
Marlene Faria

FINANCIAL DETAILS

Support type
Non-Refundable

Maximum Funding Rate
100%

Budget
7.7M€

Eligible Project Value
3.8M€ - 3.8M€

DATES & DEADLINES

Publication Date
December 12, 2025

Opening Date
May 5, 2027

Deadline
November 4, 2027 at 05:00 PM GMT+1

DESCRIPTION

Objectives

This call aims to enhance the security and resilience of critical infrastructure in the EU by addressing the risks posed by the malicious use of Open-Source Intelligence (OSINT). The objective is to improve awareness among critical infrastructure operators and authorities about OSINT threats, develop advanced tools for OSINT mapping and risk analysis, and strengthen incident response and business continuity planning. The call also seeks to support the removal of harmful OSINT from the public domain and to develop awareness campaigns and training for employees of critical entities. Eligible applicants include consortia with at least three relevant practitioners from EU Member States or Associated Countries, representing critical infrastructure operators, authorities responsible for resilience, or law enforcement/private security companies. Entities established in China or controlled by Chinese entities are not eligible.

Funding

The support is provided as a non-refundable grant under the Horizon Innovation Actions (IA) scheme. The funding rate is up to 70% of eligible costs for most participants, and up to 100% for non-profit legal entities. The total budget for the topic is €7.67 million, with an expected EU contribution of €3.835 million per project and two grants anticipated. Eligible costs are reimbursed as a lump sum.

ELIGIBLE EXPENSES

- Personnel Costs
- Travel costs
- Equipment costs
- Other goods, works and services costs
- Subcontracting
- Indirect Costs

BONUSES & MAJORATIONS

- Up to 100% funding rate for non-profit legal entities
- Mandatory involvement of at least 3 relevant practitioners from EU/Associated Countries
- Synergy-building and clustering with other relevant projects encouraged

ELIGIBILITY

Application Mode
Consortium / Copromotion

Eligible Sectors

- Energy & Environment
- ICT & Software
- Logistics
- Other

Company Typologies

- Micro
- SME
- Small Mid-Cap
- Mid-Cap
- Large
- Private non-profit entities
- Public entities

Action Types

- Development of OSINT mapping and risk analysis tools
- Analysis of publicly available information for hostile operations
- Development of awareness campaigns and training curricula
- Incident response and business continuity model improvement
- Removal of harmful OSINT from public domain
- Integration and optimisation of existing security tools
- Engagement with Europol Innovation Lab for validation
- Consideration of AI data processing implications for OSINT misuse
- Development of tools to counter hybrid and lone wolf threats

EU PROGRAMME DETAILS

Call ID	Cluster
HORIZON-CL3-2027-01-INFRA-02	Cluster 3: Civil Security for Society
Destination	Submission Mode
D3. Resilient Infrastructure	single-stage
EU Contribution	Expected Projects
€3,835,000.00 per project	2
Funding Rate Rule	
Up to 70% of eligible costs for Innovation Actions (IA); up to 100% for non-profit legal entities	

OFFICIAL LINKS

Official Regulation

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-CL3-2027-01-INFRA-02>

Grantavia page

<https://grantavia.com/en/incentives/impact-of-malicious-use-of-open-source-intelligence-on-critical-infrastructure-business-continuity>

Information Video

<https://www.youtube.com/shorts/46sBAgRpL5o>

Schedule a meeting

<https://calendly.com/filipa-silva-epsa/reuniao>