

Seeking security practitioners for an EU-funded call on infrastructure resilience and crisis management

Summary

Profile type	Company's country	POD reference
Research & Development Request	France	RDRFR20250912002
Profile status	Type of partnership	Targeted countries
PUBLISHED	Research and development cooperation agreement	• World
Contact Person	Term of validity	Last update
Enrico FRANZIN	12 Sep 2025 12 Sep 2026	12 Sep 2025

General Information

Short summary

Coordinator: French SME, crisis platforms and decision support. Objective: co-develop capabilities to detect cascading risks early, analyze faster, and coordinate cross-border; fuse ops with data; test interdependencies. Partners: EU/assoc. CI ops (energy, water, health, transport, telecom), regulators/cyber agencies/city resilience, civil protection, law enforcement/private CI security. Role: co-define needs, join pilots, provide scenarios/data/feedback, support uptake.

Full description

Overview and why Modern utilities (energy, water, transport, telecoms) are tightly connected. A disturbance in one can cascade into others and across borders. Data is fragmented, and coordination is hard under time pressure. Our project will research and develop practical, standards-based capabilities that: - builds a shared, cross-sector operational picture from selected operational data and open geospatial sources, - runs tests to anticipate knock-on effects, and - offers explainable decision support and alerting for multi-agency/multi-jurisdiction response. With whom A core consortium of industrial and academic partners from France, Denmark, Spain, Portugal, and Greece (crisis platforms, Earth observation, AI/analytics, risk modelling, exercises and human factors). We are now adding security practitioners to co-design, test and validate. Programme framework Horizon Europe, Cluster 3 (Civil Security for Society), topic HORIZON-CL3-2025-01-INFRA-01 (Innovation Action). Proposal submission planned November 2025; project start expected mid-2026, subject to EU evaluation. Timescale: Planned 36 months. Type and role of

partners sought - CI operators: operational processes, incident handling, safe data provision (non-sensitive or synthetic where needed), site access for table-tops/drills, evaluation of decision-support outputs. - Resilience authorities: risk and regulatory context, inter-agency procedures, data-sharing constraints, validation of cross-border workflows. - Civil protection: exercise planning, evacuation/protected-route logistics, public messaging, after-action reviews. - Law enforcement / private security: traffic control, convoy escort, public order, cyber incident cooperation, misinformation counter-measures, and communications. - All partners help shape scenarios, define KPIs, test prototypes, and contribute to lessons learned and uptake plans.

Advantages and innovations

1. EU- based capabilities 2. Federated, privacy-preserving set-up 3. Stress testing of interdependencies 4. Explainable decision support 5. Standards-first interoperability 6. Practitioner-led validation

Technical specification or expertise sought

- EU or associated country organisation; ability to sign an NDA and a Horizon Europe Grant Agreement if selected - Potential actor of complex crisis scenarios - Appoint a single point of contact and a small core team (operational lead + technical contact) - Willingness to take part in requirements workshops, table-top exercises, pilot activities, and structured evaluations (surveys/interviews) - Ability to share non-sensitive operational data, de-identified samples, or synthetic data; alternatively to provide expert ground truth and process descriptions if real data cannot be shared - Readiness to contribute to dissemination and exploitation (non-confidential case stories, policy inputs, standardisation feedback)

Stage of development

Under development

Sustainable Development goals

- **Goal 17: Partnerships to achieve the Goal**
- **Goal 13: Climate Action**
- **Goal 11: Sustainable Cities and Communities**
- **Goal 9: Industry, Innovation and Infrastructure**

IPR Status

Secret know-how

IPR Notes

Partner Sought

Expected role of the partner

Co-define needs, join pilots, provide scenarios/data/feedback, support uptake

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **SME <=10**
- **SME 11-49**
- **Other**
- **Big company**
- **SME 50 - 249**

Call Details

Framework program

Horizon Europe

Call title and identifier

HORIZON-CL3-2025-01-INFRA-01 "Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures"

Submission and evaluation scheme

Anticipated project budget

5000000

Coordinator required

No

Deadline for EoI

11 Nov 2025

Deadline of the call

12 Nov 2025

Project duration in weeks

156

Web link to the call

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/to-pic-details/HORIZON-CL3-2025-01-INFRA-01?>

Project title and acronym

Dissemination

Technology keywords

Targeted countries

- **World**

Market keywords

- **01004002 - Data communication components**
- **06007001 - Other energy production**
- **08005 - Other Industrial Products (not elsewhere classified)**

Sector groups involved

- **Energy-Intensive Industries**
- **Renewable Energy**
- **Aerospace and Defence**
- **Mobility - Transport - Automotive**
- **Agri-Food**
- **Maritime Industries and Services**
- **Health**