EU Security research in support to Critical Infrastructure Protection

Christoph Castex

European Commission
DG Migration and Home Affairs
Directorate B: Migration and Mobility
unit B4: Innovation and industry for Security

General information on the call/topic

Call:

Critical infrastructure protection

Topic:

CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

Budgetary overview

Topics (Type of Action)	Budgets (EUR million)		Deadlines
	2016	2017	
Opening: 15 Mar 2016			
CIP-01-2016-2017 (IA)	20.00		25 Aug 2016
Opening: 01 Mar 2017			
CIP-01-2016-2017 (IA)		20.00	24 Aug 2017
Overall indicative budget	20.00	20.00	

Eligibility criteria

At least **2 operators** of the chosen type of critical infrastructure operating in **2 countries** must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of **industry able to provide security** solutions is required.

Mandatory eligibility criteria

Why do we apply these?

- **Enhance policy support**
- **Improve market uptake**
- **Increase Innovation dimension**
- **Reduce oversubscription**
- **Reduce duplications**

Technical aspects

- TRL 7 – system prototype demonstration in operational environment.
- The participation of SMEs is strongly encouraged.
- International cooperation in research and innovation.
- Indicative budget: of € 8million.
- A maximum of one project will be selected per critical infrastructure.

Scope and policy background

The reasoning behind the CIP call

The lines between the physical and the cyber world are increasingly blurred. Nearly everything is connected to the internet. Threats cannot be analysed solely as physical or cyber.

Exclusive list of CI

- ~~Water Systems~~,
- ~~Energy Infrastructure (power plants and distribution);~~
- ~~Transport Infrastructure and means of transportation;~~
- Communication Infrastructure;
- Health Services;
- Financial Services.

Scope

- Prevention, detection, response, and in case of failure, mitigation of consequences over the life span of the infrastructure
- All aspects of both physical and cyber threats and incidents, but also systemic security management issues, interconnections, and cascading effects.
- Sharing information with the public in the vicinity of the installations, protection of rescue teams, security teams and monitoring teams.

Expected Impact – main points

Short term:

Analysis of physical/cyber detection technologies as well as vulnerabilities.

Mid term:

Tested solutions to prevent, detect, respond and mitigate physical and cyber threats.

Long term:

Convergence of safety and security standards, and the pre-establishment of certification mechanisms.

BES

Border Security and External Security

Development of technologies, capabilities and solutions to:

Improve EU border security*:*

- *Flow of people: research will support the exploitation of the potential given by the European Border Surveillance System (**EUROSUR** - Regulation No 1052/2013) and promote an enhanced use of new technology for border checks in relation to the SMART BORDERS legislative initiative* ***(DG HOME)***
- *Flow of goods: research will address, in the context of the EU's customs policy, supply chain security trying to strike the right balance with trade facilitation* ***(DG TAXUD)***

Support the EU External Security Policies in civilian tasks (EEAS)

SEC-13-BES-2017: Next generation of information systems to support EU external policies

Scope:

- *This topic is to support the development of a cost-effective common Situational Awareness, Information Exchange and Operation Control Platform.*

Expected Impact:

- *Solid basis for a full-scale, cost-effective common situational awareness, information exchange and operation control platform for EU civilian external actions.*
- *Improved management of EU resources' allocated to EU civilian external actions.*

Type of Action: Pre-Commercial Procurement (max 10M) TRL 8

Supporting European Civilian External Actions (CIVILEX)

http://civilex.eu

Coordinator ATOS SPAIN SA

Project Overview

CIVILEX aims to identify, characterise and model the communication and information systems in use within the EU civilian missions, understand the stakeholders' requirements and the institutional context in which changes need to happen and provide possible solutions to be tackled by a future interoperable Situational Awareness, Information Exchange and **O**peration **C**ontrol **P**latform (**OCP**).

A common understanding and situational awareness about crisis management in EU civilian external actions will be enhanced since CIVILEX will pave the way for such an infrastructure to be procured and implemented after the termination of the CIVILEX project. The implementation of an OCP would also contribute to making the EU external action in crisis situations more coordinated and more comprehensive in line with the objectives of the EU's policy to promote a comprehensive approach.

The objectives of the project are to:

1. Create understanding and commitment on the institutional changes that would help to streamline information management within CSDP missions,
2. Analyze the status quo of information management, exchange and operational control and identify the technical, security and usability requirements for the formulation of appropriate technical solutions,
3. Review the state-of-the-art technologies and applications for effective information exchange and identify options for future technical interoperability formats, architecture and information exchange solutions and,
4. Provide recommendations for setting the research and procurement agenda for acquisition and implementation of the future OCP, taking into account the technical options and institutional dimensions.

General considerations

To ensure that outcome of the PCP action becomes also available to EU Member States national authorities as well as EU agencies not participating in the PCP for further procurement purposes, the proposal must necessarily state:

(1). Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product fully or partly derived from the PCP action, the use of the information required to run such a procurement process, and solely for that purpose.

(2). Commitment from participating procurement authorities to consult with any legal entity generating information to be released for the purpose set out in (1), unless contrary to applicable legislation.

(3). Commitment from participating procurement authorities to negotiate the use granted under (1) on Fair Reasonable and Non-Discriminatory (FRAND) terms.

The respective option on additional exploitation obligations of Article 28.1 of the Model Grant Agreement will be applied.

Thank you for your attention !

More information:
http://ec.europa.eu/dgs/home-affairs/financing/fundings/research-for-security/index_en.htm

The Work Programme:
http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf