FP7-SEC-2013-1

Call identifier: FP7-SEC-2013-1

Date of publication: 10/July/2012

Deadline: 22/November/2012 at 17.00.00, Brussels local time[1]

Indicative budget: EUR 299.33million[2]

The budget for this call is indicative. The final budget awarded to actions implemented through calls for proposals may vary:

- An indicative 45% (deviation possible from 35% to 65%) of the budget for topics to be implemented through Integration Projects and Demonstration Projects Phase II (large scale integrating projects).
- An indicative 6% (deviation possible from 0% to 10%) for Pre-Operational-Validation topic 3.2-1 and for Pre-Operational-Validation topic 5.3-2.
- An indicative 49% (deviation possible from 39% to 69%) of the budget for the other topics (small or medium-scale focused research project and coordination and support actions).
- Within the above indicated limits, up to 5% can be used for the open topics for SMEs 7.2-1 and 7.6-1.
- Within the above indicative limits, up to 1% can be used for international cooperation partners within selected projects.
- Any repartition of the call budget may also vary by up to 10% of the total value of the indicated budget for the call.

[1] The Director-General responsible may delay this deadline by up to two months.

[2] Under the condition that the draft budget for 2013 is adopted without modification by the budgetary authority.

Topics called:

Activity/ Area	**Topics called**	**Funding Schemes**
Activity 10.1 Security of citizens		
Area: 10.1.1 Organised crime	Topic SEC-2013.1.1-1 Serious organised economic crime	CP-IP
	Topic SEC-2013.1.1-2 “Stronger Identity for EU citizens”	CP-FP
Area: 10.1.2 Intelligence against terrorism	none	none
Area: 10.1.3 Explosives	Topic SEC-2013.1.3-1 Inhibiting the use of explosives precursors	CP-FP
Area: 10.1.4 Ordinary crime and forensics	Topic SEC-2013.1.4-1 Smart and protective clothing for law enforcement and first responders	CP-FP
	Topic SEC-2013.1.4-2 Development of a Common European Framework for the application of new technologies in the collection and use of evidence	CSA (Supporting Action)
Area: 10.1.5 CBRN protection	Topic SEC-2013.1.5-1 European toolbox, focusing on procedures, practices and guidelines for CBRN forensic aspects	CP-FP
Area: 10.1.6 Information gathering	Topic SEC-2013.1.6-1 Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes	CP-IP
	Topic SEC-2013.1.6-2 Novel technologies and management solutions for protection of crowds	CP-IP
	Topic SEC-2013-1.6-3 Surveillance of wide zones: from detection to alert	CP-IP
	Topic SEC-2013-1.6-4 Information Exploitation	CP-IP
Activity: 10.2 Security of infrastructures and utilities		

Area: 10.2.1 Design, planning of buildings and urban areas	Topic SEC-2013.2.1-1 Evidence based and integral security concepts for government asset protection	CP-FP
	Topic SEC-2013.2.1-2 Impact of extreme weather on critical infrastructure	CP-FP
Area: 10.2.2 Energy, transport, communication grids	Topic SEC-2013.2.2-1 A research agenda for security issues on land transport	CSA (Coordinating Action)
	Topic SEC-2013.2.2-2 Toolbox for pandemics or highly dangerous pathogens in transport hubs – Capability Project	CP-FP
	Topic SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks	CP-FP
	Topic SEC-2013.2.2-4 Cost effectiveness of security measures applied to renewable/distributed energy production and distribution	CP-FP
	Topic SEC-2013.2.2-5 Security of ground based infrastructure and assets operating space systems	CP-FP
Area: 10.2.3 Surveillance	none	none
Area: 10.2.4 Supply chain	Topic SEC-2013.2.4-1 Phase II demonstration programme on logistics and supply chain security	CP-IP
	Topic SEC-2013.2.4-2 Non-military protection measures for merchant shipping against piracy	CP-FP or Coordination and Support Action (Coordinating Action)
Area: 10.2.5 Cyber crime	Topic SEC-2013.2.5-1 Developing a Cyber crime and cyber terrorism research agenda	CSA (Coordinating Action)
	Topic SEC-2013.2.5-2 Understanding the economic impacts of Cyber crime in non-ICT sectors across jurisdictions	CP-FP

	Topic SEC-2013.2.5-3 Pan European detection and management of incidents/attacks on critical infrastructures in sectors other than the ICT sector (i.e. energy, transport, finance, etc)	CP-IP
	Topic SEC-2013.2.5-4 Protection systems for utility networks	CP-FP
Activity: 10.3 Intelligent surveillance and border security		
Area: 10.3.1 Sea borders	none	none
Area: 10.3.2 Land borders	Topic SEC-2013.3.2-1 Pre-Operational Validation (POV) on land borders	CP-CSA
	Topic SEC-2013.3.2-2 Sensor technology for under foliage detection	CP-IP
	Topic SEC-2013.3.2-3 Mobile equipment at the land border crossing points	CP-FP
Area: 10.3.3 Air borders	none	none
Area: 10.3.4 Border checks	Topic SEC-2013.3.4-1 Border checkpoints - hidden human detection	CP-FP
	Topic SEC-2013.3.4-2 Extended border security - passport breeder document security	CSA (Supporting Action)
	Topic SEC-2013.3.4-3 Security checks versus risk at borders	CP-FP
Area: 10.3.5 Intelligent border surveillance	none	none
Activity: 10.4 Restoring security and safety in case of crisis		
Area: 10.4.1 Preparedness,	Topic SEC-2013.4.1-1 Phase II demonstration programme on aftermath crisis management	CP-IP

prevention, mitigation and planning	Topic SEC-2013.4.1-2 Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and other unfortunate consequences	CP-FP
	Topic SEC-2013.4.1-3 Development of simulation models and tools for optimising the pre-deployment and deployment of resources and the supply chain in external emergency situations	CP-FP
	Topic SEC-2013.4.1-4 Development of decision support tools for improving preparedness and response of Health Services involved in emergency situations	CP-FP
	Topic SEC-2013.4.1-5 Preparing societies to cope with large scale and/or cross border crisis and disasters	CSA (Supporting Action)
	Topic SEC-2013.4.1-6 Preparedness for and management of large scale forest fires	CP-IP
Area: 10.4.2 Response	Topic SEC-2013.4.2-1 Fast rescue of disaster surviving victims: Simulation of and situation awareness during structural collapses including detection of survivors and survival spaces	CP-IP
Area: 10.4.3 Recovery	Topic SEC-2013.4.3-1 Shaping immediate relief action in line with the goals of development co-operation in post crisis / post conflict societies to maintain stability	CP-FP
Area: 10.4.4 CBRN response	Topic SEC-2013.4.4-1 Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination	CP-IP
Activity: 10.5 Security systems integration, interconnectivity and interoperability		
Area: 10.5.1 Information management	Topic SEC-2013.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities	CP-FP
	Topic SEC-2013.5.1-2 Audio and voice analysis, speaker identification for security applications	CP-IP

Area: 10.5.2 Secure communications	none	none
Area: 10.5.3 Interoperability	Topic SEC-2013.5.3-1 Definition of interoperability specifications for information and meta-data exchange amongst sensors and control systems	CP-FP
	Topic SEC-2013.5.3-2 Testing the interoperability of maritime surveillance systems	CP-CSA
Area: 10.5.4 Standardisation	Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products	CP-FP
Activity: 10.6 Security and society		
Area: 10.6.1 Citizens, media and security	Topic SEC-2013.6.1-1 The impact of social media in emergencies	CP-FP
	Topic SEC-2013.6.1-2 Varying forms of terrorism	CP-FP
	Topic SEC-2013.6.1-3 Trafficking in Human Beings: analysis of criminal networks for more effective counter-trafficking	CSA (Supporting Action)
Area: 10.6.2 Organisational requirements for interoperability of public users	Topic SEC-2013.6.2-1 Facilitators for assistance among EU Member States in emergencies in the EU	CP-FP or CSA (Coordinating Action)
Area: 10.6.3 Foresight, scenarios and security as evolving concept	Topic SEC-2013.6.3-1 Horizon scanning and foresight for security research and innovation	CSA (Coordinating Action)
	Topic SEC-2013.6.3-2 The evolving concept of security	CSA (Coordinating Action)
Area: 10.6.4 Security economics	none	none

Area: 10.6.5 Ethics and justice	Topic SEC-2013.6.5-1 Synthesis of results and reviewing of ethics, legal and justice activities in Security research in FP7	CSA (Coordinating Action)
Activity: 10.7 Security Research coordination and structuring		
Area: 10.7.1 ERA-net	none	none
Area: 10.7.2 Small and Medium Enterprises	Topic SEC-2013.7.2-1 Open topic for Small and Medium Enterprises: “Solutions for frequent petty crimes that are of high impact to local communities and citizens"	CP-FP
Area: 10.7.3 Studies	Topic SEC-2013.7.3-1 Increasing the engagement of civil society in security research	CSA (Supporting Action)
Area: 10.7.4 Other coordination	Topic SEC-2013.7.4-1 Trans-national cooperation among public security research stakeholders	CSA (Coordinating Action)
Area: 10.7.5 End-users	none	none
Area: 10.7.6 Training	Topic SEC-2013.7.6-1 Open topic for Small and Medium Enterprises: “Use of serious gaming in order to improve intelligence analysis by law enforcement agents”	CP-FP

Eligibility conditions:

- The general eligibility criteria are set out in Annex 2 of this work programme, and in the guide for applicants. Please note that the completeness criterion also includes that part B of the proposal shall be readable, accessible and printable.

Funding scheme	**Minimum conditions**
Collaborative Projects	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (coordinating action)	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (supporting action)	At least 1 independent legal entity.

- Only information provided in part A of the proposal will be used to determine whether the proposal is eligible with respect to budget thresholds and/or minimum number of eligible participants.

- Proposals containing any classified information shall be ineligible.

Additional eligibility criterion:

Topics SEC-2013.3.2-1 and SEC-2013.5.3-2 will require the participation of at least 3 independent public authorities (at either local, regional, national or supra-national level) no 2 of which are established in the same MS or AC (documents proving the status of the participant have to be provided).

Evaluation criteria for evaluating POV proposals

1. Scientific and/or technological excellence

   - Progress beyond the state-of-the-art.

   - Quality and effectiveness of the S/T methodology and associated strategy and work plan.

2. Quality and efficiency of the implementation and the management

   - Quality of the consortium as a whole (including complementarity, balance).

   - Commitment of participating authorities.

   - Appropriateness of the allocation and justification of the resources to be committed (staff, equipment,…).

3. The potential impact through the development, dissemination and use of project results

   - Appropriateness of measures for the dissemination and/or exploitation of project results, and management of intellectual property.

Evaluation procedure:

- The evaluation criteria and scoring scheme are set out in annex 2 of the work programme.

- Proposal page limits: Applicants must ensure that proposals conform to the page limits and layout given in the Guide for Applicants, and in the proposal part B template available through the electronic Submission Services of the Commission .

The Commission may instruct the experts to disregard any pages exceeding these limits.

The minimum font size allowed is 11 points. The page size is A4, and all margins (top, bottom, left, right) should be at least 15 mm (not including any footers or headers).

- A one-stage submission and evaluation procedure will be used.
- Experts will carry out the individual evaluation of proposals remotely.
- The procedure for prioritising proposals with equal scores is described in annex 2 of the work programme.

Particular requirement for participation, evaluation and implementation:

Classified Information

Proposals must not contain any *classified information* (note that the proposed action itself *can* involve classified information). If classified inputs are required to carry out a proposed action or the output of the action needs to be classified, proposers have to ensure the following:

- provide evidence of the clearance of all relevant facilities;
- clarify issues such as e.g. access to classified information or export or transfer control with the National Security Authorities (NSA) of their Member States / Associated Countries, and provide evidence of the prior agreement of their NSAs;
- provide a Security Aspect Letter (SAL), indicating the levels of classification required at deliverables/partners level.

Absence of any of these elements may lead the Commission to decide not to proceed to negotiation of a grant agreement even if the proposal is evaluated positively. Furthermore, appropriate arrangements have to be included in the consortium agreement.

If the proposal is evaluated positively and invited for the negotiation, a definitive version of the SAL and of the SCG will be annexed to the Description of Work and must be worked out during negotiations. Special clauses will be introduced in the Grant Agreement. National security authorities will be consulted after the evaluation and before the negotiation through their representatives in the Security Assessment ad-hoc group from the Security Programme Committee. They will have the possibility to make recommendations regarding ‘classified information’ issues to be taken into account during the negotiation.

For projects based on proposals which did not contain SAL but that have been subject to security recommendations following the above procedure, a SAL and its SCG annex could be required during the negotiations.

Ethical Review

Proposed activities shall be carried out in compliance with fundamental ethical principles. If ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity. In addition, the potential impact of the resulting technologies and activities on Fundamental Rights, ethical principles and societal values should be addressed as part of the proposed research.

Small and Medium Enterprises (SME) and end-users

Consortia are strongly encouraged to actively involve *SMEs and end-users*.

Evaluation

The *evaluation criteria* (including weights and thresholds) and sub-criteria, together with the eligibility, selection and award criteria for the different funding schemes are set out in Annex 2 to this work programme.

Coordinators of all integration project proposals and of all demonstration projects (phase II) proposals that pass all the evaluation thresholds may be invited to a *hearing*.

As a result of the evaluation, a ranked list of proposals retained for funding will be drawn up as well as a reserve list of proposals that may be funded in case budget becomes available during negotiations.

Positively evaluated proposals involving sensitive and classified information, those involving international co-operation as well as those collaborative projects where 75% funding for all participants is foreseen will be flagged to the members of the *Security Programme Committee* configuration and dealt with according to its Rules for Procedure.

Indicative timetable:

This call in 2012 invites proposals to be funded in 2013. Evaluation of proposals is foreseen to be carried out in January/February 2013. It is expected that the grant agreement negotiations for the short listed proposals will be opened in the first half of 2013.

Consortia agreements are required for *all* action.

The forms of grants and maximum reimbursement rates which will be offered are specified in Annex 3 to the Cooperation work programme.

Proposers claiming that their proposal should receive EU funding for research activities up to 75% for specific reasons as described on page 10 of this document should demonstrate in the proposal that the exceptional required conditions apply.

Flat rates to cover subsistence costs:

In accordance with Annex 3 of this work programme, this call provides for the possibility to use flat rates to cover subsistence costs incurred by beneficiaries during travel carried out within grants for indirect actions. For further information, see the relevant Guides for Applicants for this call. The applicable flat rates are available on the Participant Portal at: https://ec.europa.eu/research/participants/portal/page/fp7_documents under 'Guidance documents for FP7/Financial issues/Flat rates for daily allowances.