# Call title: FP7-SEC-2012-1

- **Call identifier**: **FP7-SEC-2012-1**
- **Date of publication**: 20/July/2011
- **Deadline**: 23/November/2011 at 17.00.00, Brussels local time [1]
- **Indicative budget**: Total call budget EUR 241.7 million [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 55%) of the budget for topics to be implemented through Integration Projects and Demonstration Projects.
  - An indicative 55% (deviation possible from 45% to 65%) of the budget for the other topics.
  - Within the above indicative limits, up to 3% can be used for international cooperation partners within selected projects; an indicative limit of up to 5% can be used for SMEs in the topic 7.2-1 and an indicative limit of up to 4% can be used for the Pre-Operational-Validation topic set out in topic 3.1-2.The final budget of the call may vary by up to 10% of the total value of the indicated budget for each call; and
  - Any repartition of the call budget may also vary by up to 10% of the total value of the indicated budget for the call.

**Topics called**:

| Activity/ Area | **Topics called** | **Funding Schemes** |
|---|---|---|
| **Activity: 10.1 Increasing the Security of the Citizens** | | |
| Area: 10.1.1<br>Organised crime | None | |
| Area: 10.1.2<br>Intelligence against terrorism | None | |
| Area: 10.1.3<br>Explosives | SEC-2012.1.3-1 Less than Lethal Handling of PBIEDs | CP-FP |
| | SEC-2012.1.3-2 Home made explosives (HMEs) and recipes characterisation | CP-FP |
| Area: 10.1.4<br>Ordinary Crime and Forensic | None | |
| Area: 10.1.5<br>CBRN Protection | SEC-2012.1.5-1 CBRNE Demo Phase II | CP-IP |
| | SEC-2012.1.5-2 Improving drinking water security management and mitigation in large municipalities | CP-FP |

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

[2] Under the condition that the draft budget for 2012 is adopted without modification by the budgetary authority.

| | | |
|---|---|---|
| | against major deliberate, accidental or natural CBRN-related contaminations | |
| | SEC-2012.1.5-3 Identification and development of low-risk alternatives to high-risk chemicals | CP-FP or CSA |
| | SEC-2012.1.5-4 Securing the food chains from primary production and animal feeds to consumer ready food against deliberate, accidental or natural CBRN contamination | CP-FP |
| Area: 10.1.6<br>Information Gathering | SEC-2012.1.6-1 Digital, miniaturised operational tool for investigation | CP-FP |
| **Activity: 10.2 Security of infrastructures and utilities** | | |
| Area: 10.2.1<br>Design, planning of buildings and urban areas | SEC-2012.2.1-1 Resilience of large scale urban built infrastructure | CP-FP |
| | SEC-2012.2.1-2 Criticality analysis of critical infrastructure including concepts for forgery proof and efficient facility access systems | CP-FP |
| Area: 10.2.2<br>Energy, Transport, communication grids | SEC-2012.2.2-1 Identification of measures to counter illegal export of metal-bearing waste | CSA |
| | SEC-2012.2.2-2 Air traffic Management/Control threat assessment model | CP-IP |
| | SEC-2012.2.2-3 Improving security in air cargo transport | CP-IP |
| | SEC-2012.2.2-4 A common EU aviation security requirement to reduce costs and facilitate passenger flows | CSA |
| Area: 10.2.3<br>Surveillance | SEC-2012.2.3-1 Early warning security systems: physical protection of critical buildings | CP-FP |
| Area: 10.2.4<br>Supply chain | SEC-2012.2.4-1 Pre-normative technology development for improved and more efficient security of the supply chain | CSA |
| Area: 10.2.5<br>Cyber crime | SEC-2012.2.5-1 Convergence of physical and cyber security | CP-FP |
| | SEC-2012.2.5-2 Cyber resilience – Secure cloud computing for critical infrastructure | CP-FP |
| **Activity: 10.3 Intelligent surveillance and border security** | | |
| Area: 10.3.1<br>Sea borders | SEC-2012.3.1-1 Increasing trustworthiness of vessel reporting systems | CP-FP |
| | SEC-2012.3.1-2 Pre-Operational Validation (POV) at EU level of common application of Surveillance | CP-CSA |

| | | |
|---|---|---|
| | tools | |
| Area: 10.3.2<br>Land borders | None | |
| Area: 10.3.3<br>Air borders | None | |
| Area: 10.3.4<br>Border checks | SEC-2012.3.4-1 Research on "automated" comparison of x-ray images for cargo scanning with reference material (use of historic images in an automated environment) to identify irregularities | CP-FP |
| | SEC-2012.3.4-2 Research and validation for sub-surface fingerprint live scanners | CP-FP |
| | SEC-2012.3.4-3 Tools and processes for assessing the impact of policies/actions on border control | CSA |
| | SEC-2012.3.4-4 Innovative, cost-efficient and reliable technology to detect humans hidden in vehicles/closed compartments | CP-FP |
| | SEC-2012.3.4-5 Further research, development and pilot implementation of Terahertz passive detection techniques (T-Ray) | CP-FP |
| | SEC-2012.3.4-6 Enhancing the workflow and functionalities of Automated Border Control (ABC) gates | CP-IP |
| Area: 10.3.5<br>Border intelligent surveillance | SEC-2012.3.5-1 Development of airborne sensors and data link | CP-IP |
| **Activity: 10.4 Restoring security and safety in case of crisis** | | |
| Area: 10.4.1<br>Preparedness, prevention, mitigation and planning | SEC-2012.4.1-1 Preparedness for and management of large scale fires | CP-IP |
| | SEC-2012.4.1-2 Psycho social support in Crisis Management | CP-FP |
| Area: 10.4.2<br>Response | SEC-2012.4.2-1 Positioning and timing tools to guarantee security assets trace & tracking together with worker safety in a secure environment | CP-FP |
| | SEC-2012.4.2-2 Situational awareness guidance and evacuation systems for large crowds, including crowds unpredictable behaviour | CP-IP |
| | SEC-2012.4.2-3 Post crisis lesson learned exercise | CSA |
| Area: 10.4.3<br>Recovery | SEC-2012.4.3-1 Next generation damage and post-crisis needs assessment tool for reconstruction and | CP-FP |

| | | |
|---|---|---|
| | recovery planning | |
| Area: 10.4.4<br>CBRN Response | SEC-2012.4.4-1 Development of mobile laboratories, structures and functions to support rapid assessment of CBRN events with a cross-border or international impact | CSA |
| | SEC-2012.4.4-2 Means of decontamination of large groups, urban/wide areas and large, complex and/or sensitive object | CP-FP |
| | SEC-2012.4.4-3 Tools for detection, traceability, triage and individual monitoring of victims after a mass contamination | CP-IP |
| **Activity: 10.5 Security systems integration, interconnectivity and interoperability** | | |
| Area: 10.5.1<br>Information Management | None | |
| Area: 10.5.2<br>Secure Communications | SEC-2012.5.2-1 Preparation of the next generation of PPDR communication network | CP-FP |
| Area: 10.5.3<br>Interoperability | SEC-2012.5.3-1 Embedded protection of security systems and anti-tampering technologies | CP-FP |
| | SEC-2012.5.3-2 Establishment of a first responders platform for interoperability | CSA |
| | SEC-2012.5.3-3 Establishment of a interoperability platform/centre for testing and validating decision and intelligence systems | NoE |
| | SEC-2012.5.3-4 Global solution for interoperability between first responder communication systems | CP-IP |
| Area: 10.5.4<br>Standardisation | None | |
| **Activity: 10.6 Security and society** | | |
| Area: 10.6.1<br>Citizens, media and security | SEC-2012.6.1-1 Methodologies to assess the effectiveness of measures addressing violent radicalisation | CP-FP or CSA |
| | SEC-2012.6.1-2 Tools and methodologies, definitions and strategies for privacy by design for surveillance technologies, including ICT systems | CP-FP or Coordination and Support Action |
| | SEC-2012.6.1-3 Use of new communication/social media in crisis situations | CP-FP or Coordination and Support Action |
| Area: 10.6.2<br>Organisational requirements for interoperability of public | None | |

| | | |
|---|---|---|
| users | | |
| Area: 10.6.3<br>Foresight, scenarios and security as an evolving concept | SEC-2012.6.3-1 Developing an efficient and effective environmental scanning system as part of the early warning system for the detection of emerging organised crime threats | CP-FP |
| | SEC-2012.6.3-2 Criteria for assessing and mainstreaming societal impacts of security research activities | CSA |
| Area: 10.6.4<br>Security economics | SEC-2012.6.4-1 Fight against corruption | CSA |
| Area: 10.6.5<br>Ethics and Justice | SEC-2012.6.5-1 Legitimacy and effectiveness of legal measures against security threats | CP or CSA |
| **Activity: 10.7 Security Research coordination and structuring** | | |
| Area: 10.7.1<br>ERA-Net | None | |
| Area: 10.7.2<br>Small and Medium Enterprises | SEC-2012.7.2-1 Open topic for Small and Medium Enterprises: "Advancing contemporary forensic methods and equipment" | CP-FP |
| Area: 10.7.3<br>Studies | None | |
| Area: 10.7.4<br>Other coordination | SEC-2012.7.4-1 Coordination of national research programmes in the area of security research | CSA |
| | SEC-2012.7.4-2 Networking of researchers for a high level multi-organisational and cross-border collaboration | NoE |
| Area: 10.7.5<br>End users | None | |
| Area: 10.7.6<br>Training | None | |

- **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.

  - Table of standard minimum number of participating legal entities for all funding schemes used in the call, in line with the Rules for Participation and in the below format:

| **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 |
| Network of Excellence | 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 the minimum number of eligible participants.

- Proposals containing any classified information shall be declared ineligible.

- **Additional eligibility criterion**:
  Topic "SEC-2012.3.1-2 Pre-Operation Validation (POV) at EU level of common application of surveillance tools" requires the participation of at least 3 independent public authorities in charge of border surveillance (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 procedure**:
  - The evaluation criteria and scoring scheme are set out in Annex 2 to 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 EPSS.

    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 procedure will be followed.

  - Proposals will be evaluated in a single-step procedure.

  - Experts will carry out the individual evaluation of proposals remotely.

  - The procedure for prioritising proposals with equal scores is described in Annex 2 to the work programme.

- **Indicative timetable**: This call in 2011 invites proposals to be funded in 2012. Evaluation of proposals is foreseen to be carried out in January/February 2012. It is expected that the grant agreement negotiations for the short listed proposals will be opened in the first half of 2012.

- **Consortia agreements** are required for *all* action**.**

- **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.

- **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 8 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 to 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 at the following website: http://cordis.europa.eu/fp7/find-doc_en.html under 'Guidance documents/Flat rates for daily allowances'.