

# Informationsbrief zur Sicherheitsforschung: Hintergründe 2/11

## Informationen zum 5. Call im europäischen Sicherheitsforschungsprogramm

Der zu aktuellen Anlässen erscheinende Informationsbrief zur zivilen Sicherheitsforschung richtet sich an Unternehmen, Forschungseinrichtungen und Endnutzer. Er informiert in knapper Form über Neuigkeiten (Förderbekanntmachungen, Veranstaltungshinweise etc.) im Zusammenhang mit dem nationalen Programm „Forschung für die zivile Sicherheit“ und der europäischen Sicherheitsforschung im 7. Forschungsrahmenprogramm. Bei Bedarf werden ausführliche Informationen zu aktuellen Themen im „Informationsbrief zur Sicherheitsforschung: Hintergründe“ aufbereitet.

Der Informationsbrief wird im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) von der VDI Technologiezentrum GmbH, Projektträger Sicherheitsforschung, herausgegeben.

Eine Möglichkeit, diesen Informationsbrief kostenfrei zu abonnieren, finden Sie unter: [Abo-Informationsbrief](#).

Sehr geehrte Damen und Herren,

am 20. Juli 2011 wurde der 5. Call (FP7-SEC-2012-1) im europäischen Sicherheitsforschungsprogramm veröffentlicht. Im heutigen „Informationsbrief zur Sicherheitsforschung: Hintergründe“ haben wir für Sie die wesentlichen Informationen zusammengestellt, um Ihnen einen schnellen Überblick über die Inhalte und Rahmenbedingungen des Calls zu geben:

- **Wichtige Neuerungen**
- **Überblick über die Themen und den Zeitplan**
- **Informationen zu Förderinstrumenten und zur Einreichung von Projektvorschlägen**
- **Wissenswertes zum Projektantrag**
- **Partnersuche**
- **Aufruf zur Eintragung als Gutachter**
- **Ansprechpartner in der Nationalen Kontaktstelle Sicherheitsforschung**

### Wichtige Neuerungen

#### Arbeitsprogramm

Im Rahmen der Erstellung des 5. Calls wurden der einleitende Text und die Struktur des Arbeitsprogramms überarbeitet. Daher möchten wir potenziellen Antragstellerinnen und Antragstellern raten, diese Texte aufmerksam zu lesen. Im Folgenden sind die wesentlichen Änderungen dargestellt:

- Falls nicht anders in der Beschreibung des Topics vermerkt, ist das Topic in seiner gesamten Breite zu adressieren (siehe hierzu Seite 14 des Arbeitsprogramms).
- Die ethischen, (datenschutz-)rechtlichen und gesellschaftlichen Fragestellungen werden in der europäischen Sicherheitsforschung nun noch stärker betont. Relevante Fragestellungen sollen in

jedem Antrag, insbesondere in den Arbeitsplänen, berücksichtigt und damit in die Arbeiten einbezogen werden (siehe hierzu Seite 11 f. des Arbeitsprogramms). Darüber hinaus wird eine Vielzahl von Topics mit gesellschaftswissenschaftlichem Bezug (Aktivität 6 im Arbeitsprogramm) ausgeschrieben.

- Der Einbezug von Endnutzern in Projekte wird nun noch deutlicher hervorgehoben. Insbesondere bei großvolumigen Projekten sollte auf eine enge Endnutzereinbindung geachtet werden.
- Im Bereich Forensik wird ein offenes Topic für KMU ausgeschrieben (SEC-2012.7.2-1).
- Das Instrument Präoperationale Validierung (Pre Operational Validation, POV) wird als Pilotmaßnahme ausgeschrieben (siehe auch Förderinstrumente).
- Für die Fördervolumen der Befähigungs- und Integrationsprojekte werden nur noch Empfehlungen ausgesprochen (siehe hierzu Seite 9 des Arbeitsprogramms).

## Überblick über die Themen und den Zeitplan

### Thematische Ausrichtung

Der 5. Call im europäischen Sicherheitsforschungsprogramm beinhaltet ein Budget in Höhe von 241,7 Mio. Euro und umfasst 51 Themen, die ein breites Feld der Sicherheitsforschung abdecken:

- CBRN(E) Detektion und Dekontamination
- Cybersicherheit und Resilienz
- Evakuierungssysteme
- Schutz kritischer Infrastrukturen
- Krisenmanagement und -bewältigung
- Flughafensicherheit
- Gesellschaftliche Dimensionen
- Forensik

Eine Liste der Topics finden Sie als Auszug aus dem Arbeitsprogramm im Anhang zu diesem Dokument. Das vollständige Arbeitsprogramm mit einer ausführlichen Beschreibung der Topics können Sie im Participant Portal unter folgendem Link herunterladen:

<http://ec.europa.eu/research/participants/portal/page/cooperation?callIdentifier=FP7-SEC-2012-1>

### Demonstrationsprogramme

Im 5. Call wird das großvolumige Demonstrationsprogramm CBRNE – Phase II ausgeschrieben. Die Ausschreibung der ausstehenden Themen ist für die zukünftigen Calls wie folgt geplant:

- 6. Call – Security of Supply Chains and Logistics – Phase II
- 6. Call – Crisis Management – Phase II

Eine Darstellung des Instruments „Demonstrationsprogramm“ finden Sie unter dem Punkt „Förderinstrumente“ in diesem Informationsbrief.

## Zeitplan

Veröffentlichung: 20.07.2011  
Deadline: 23.11.2011, 17.00 Uhr (Brüsseler Ortszeit)  
Evaluation: voraussichtlich Februar 2012

Bitte beachten Sie, dass Anträge, die nach Ablauf der Deadline eingereicht werden, ungültig sind. Der 6. Call wird voraussichtlich im Juli 2012 erscheinen.

## Informationen zu Förderinstrumenten und zur Einreichung von Projektvorschlägen

### Förderinstrumente

Die Ausschreibung sieht unterschiedliche Förderinstrumente vor, die sich hinsichtlich ihrer inhaltlichen Ausrichtung und dem verfügbaren Budget unterscheiden:

– Verbundprojekte (Collaborative Project, CP): Beim Förderinstrument „Collaborative Project“ werden die folgenden drei Typen unterschieden:

- **Befähigungsprojekte** (Capability Projects, seit dem 4. Call auch als „Focused Research Projects“ bezeichnet, **CP-FP**) zielen auf die Anpassung bestehender oder die Entwicklung neuer Technologien und neuen Wissens ab. **Empfohlene Obergrenze der Fördermittel pro Projekt 3,5 Mio. Euro.** Typisches Gesamtbudget pro Projekt 2-5 Mio. Euro.
- **Integrationsprojekte** (Integration Projects, **CP-IP**) zielen auf eine Kombination von Fähigkeiten in einem Sicherheitssystem ab und zeigen dessen Leistungsfähigkeit. **Empfohlene Untergrenze der Fördermittel pro Projekt 3,5 Mio. Euro.** Typisches Gesamtbudget pro Projekt 10-25 Mio. Euro.
- **Demonstrationsprogramme** (Demonstration Programmes, DP): Während in der Phase I (**CSA-DP**) eine Roadmap entwickelt wird, zielt die Phase II (**CP-DP**) auf die Kombination von Sicherheitssystemen zu Systemen-von-Systemen ab. Diese Systeme-von-Systemen sollen eine ganzheitliche Lösung von komplexen Herausforderungen im Bereich der Sicherheit darstellen. Die Demonstrationsprogramme sollen auf europäischer Ebene wichtige Akteure aus den Bereichen Endnutzer, Industrie und Forschung zusammenbringen und gemäß der Europäischen Kommission einen starken Einfluss auf die Erschließung von neuen Märkten und die Entwicklung von Standards ausüben.

Ziel der Phase I eines Demonstrationsprogramms ist die inhaltliche Vorbereitung der Phase II durch die Erstellung einer Roadmap. Bitte beachten Sie, dass die Ausschreibung der Phase II unabhängig von der Vergabe der Phase I erfolgt, d. h. Konsortien, die in Phase I eine Roadmap erstellt haben, werden nicht automatisch in die Phase II übernommen, sondern stellen sich erneut in einer Ausschreibung dem Wettbewerb. Zwischen der Ausschreibung der Phase I und der Phase II liegen nach derzeitigem

Stand ca. 2 Jahre. Ein Projekt der Phase I wird als Coordination and Support Action (CSA) gefördert.

- Koordinierende und unterstützende Maßnahmen (Coordination and Support Action, **CSA**) resultieren in Studien und Analysen oder fördern die Vernetzung relevanter Akteure durch Seminare und Konferenzen. Innerhalb dieses Förderinstruments wird zwischen „Coordinating Action“ und „Supporting Action“ unterschieden. In beiden Fällen liegt das typische Gesamtbudget bei 0,5-1 Mio. Euro pro Projekt.
- Exzellenznetzwerke (Networks of Excellence, **NoE**) dienen zur Strukturierung und Stärkung der europäischen Forschungslandschaft.
- Präoperationale Validierung (Pre Operational Validation, **POV**) ist eine Kombination der Instrumente „Coordination and Support Action“ und „Collaborative Project“ (**CP-CSA**) und richtet sich in der ersten Ausschreibungsphase an Behörden und Organisationen mit Sicherheitsaufgaben. Falls Sie Fragen zu diesem als Pilotmaßnahme (Topic SEC-2012.3.1-2) ausgeschriebenen Instrument haben, möchten wir Sie bitten, sich direkt an die Mitarbeiter der NKS zu wenden.
- Die Angabe, welches Förderinstrument für das von Ihnen gewählte Topic gilt, finden Sie unter dem Punkt „Funding schemes“ in der Beschreibung des jeweiligen Topics.

### **Informationen zur Einreichung von Projektvorschlägen**

Die Europäische Kommission und das Bundesministerium für Bildung und Forschung stellen Ihnen Dokumente zur Verfügung, die Sie bei Ihrer Antragstellung unterstützen. Für Ihre Antragstellung gibt Ihnen der für das jeweilige Förderinstrument gültige „Guide for Applicants“ die relevanten Informationen.

Essenziell für eine Antragstellung sind folgende Dokumente:

- FP7 Factsheets
- Call Fiche
- Work Programme/Arbeitsprogramm
- Guide for Applicants (Common Part und Annexes) für das jeweilige Förderinstrument:
  - Collaborative Project (CP)
  - Coordination and Support Action: Supporting (CSA-SA)
  - Coordination and Support Action: Coordinating (CSA-CA)
  - Networks of Excellence (NoE)
  - Combined Collaborative Project and Coordination and Support Action for Pre-Operational Validation (CP-CSA)

Diese Dokumente können Sie im Participant Portal unter folgendem Link herunterladen:

<http://ec.europa.eu/research/participants/portal/page/cooperation?callIdentifier=FP7-SEC-2012-1>

Weiterhin empfehlen wir Ihnen die Lektüre folgender Dokumente:

- Antragstellung im FP7 – Leitfaden für eine erfolgreiche Beteiligung  
[http://www.forschungsrahmenprogramm.de/ media/Antragstellung7FRP\\_2Auflage.pdf](http://www.forschungsrahmenprogramm.de/media/Antragstellung7FRP_2Auflage.pdf)
- ESRAB- und ESRIF-Bericht (Hintergrundinformationen zur Sicherheitsforschung im FP7)  
[http://www.nks-security.de/files/esrab\\_report\\_en.pdf](http://www.nks-security.de/files/esrab_report_en.pdf)  
[http://www.nks-security.de/files/ESRIF\\_Final\\_Report\\_\(EN\).pdf](http://www.nks-security.de/files/ESRIF_Final_Report_(EN).pdf)

### **Wissenswertes zum Projektantrag**

Die Einreichung des Antrags kann nur elektronisch mittels des „Electronic Proposal Submission Service (EPSS)“ erfolgen: Das EPSS erreichen Sie für das jeweilige Förderinstrument wie folgt:

- Collaborative Project (Small or Medium-Scale Focused Research Project, CP-FP):  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=CP-FP](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=CP-FP)
- Collaborative Project (Large Scale Integrating Project, CP-IP):  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=CP-IP](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=CP-IP)
- Coordination and Support Action: Coordinating (CSA-CA):  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=CSA-CA](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=CSA-CA)
- Coordination and Support Action: Supporting (CSA-SA):  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=CSA-SA](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=CSA-SA)
- Networks of Excellence (NoE):  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=NoE](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=NoE)
- Combined Collaborative Project and Coordination and Support Action for Pre-Operational Validation (CP-CSA)  
[https://www.epss-fp7.org/epss/welcome.jsp?CALL\\_ID=436&SUBSCHEME\\_ID=CP-CSA](https://www.epss-fp7.org/epss/welcome.jsp?CALL_ID=436&SUBSCHEME_ID=CP-CSA)

### **Gliederung eines Projektantrags**

Der Projektantrag besteht aus zwei Teilen:

Teil A: Enthält alle administrativen Angaben über den Antrag, die Projektpartner und das Budget. Die Eingabe erfolgt mittels Online-Formular via EPSS. Genaue Erläuterungen zu den einzelnen Punkten finden Sie im Annex 3 des „Guide for Applicants“.

Teil B: Besteht aus einer Vorlage, die eine Liste von Überschriften enthält und somit die Struktur für die Darstellung des wissenschaftlichen und technischen Inhalts des Projektantrags vorgibt. Antragsteller sollten der vorgegebenen Gliederung und maximalen Seitenzahl (Annex 4 des „Guide for Applicants“) in jedem Fall folgen, da sich die Gliederung an den Evaluationskriterien orientiert.

Teil B muss als PDF-Datei via EPSS hochgeladen werden, deren Größe 10 MB nicht überschreiten darf. Diesen Teil können Sie gemäß der im Annex 4 vorgegebenen Gliederung zunächst im Word-Format vorbereiten.

Bitte beachten Sie bei der Vorbereitung Ihrer Projekte, dass die EU ausdrücklich die Einbeziehung von Endnutzern wünscht. Je nach angesprochenem Bereich können das Behörden, Polizei, Feuerwehr, Flughäfen, Betreiber von Bahnnetzen usw. sein.

Projektvorschläge, die im Rahmen dieses Aufrufs eingereicht werden, dürfen keine aus staatlicher Sicht unter Verschluss zu haltende Informationen enthalten. Während der Projektdurchführung können jedoch entsprechende Informationen erarbeitet werden bzw. in das Projekt einfließen. Nähere Informationen hierzu finden Sie unter dem Punkt „Security Sensitive Proposals“ im Annex 4 & 5 des „Guide for Applicants“.

Nehmen Sie zu jedem geforderten Gliederungspunkt Stellung und gehen Sie auf die Intention und die Charakteristika der europäischen Sicherheitsforschung im Allgemeinen und des gewählten Topic im Speziellen ein.

Verfassen Sie Ihren Antrag in einfacher, gut verständlicher englischer Sprache.

Die Mitarbeiter der nationalen Kontaktstelle Sicherheitsforschung sehen sich gern vorab Ihre Anträge an und unterstützen Sie bei der Antragserarbeitung. Bitte schicken Sie uns Ihre Projektvorschläge möglichst langfristig zu, da erfahrungsgemäß kurz vor Ablauf der Abgabefrist viele Projektideen zu begutachten sind.

### **Einbeziehung von KMU**

Neben der Beteiligung von Endnutzern ist es erwünscht, auch kleine und mittlere Unternehmen (KMU) in Projekte einzubeziehen. Darüber hinaus richtet sich ein offenes Topic im Bereich Forensik speziell an KMU. Die Europäische Kommission weist in diesem Zusammenhang darauf hin, dass als KMU nur solche Unternehmen anerkannt werden, die der folgenden Definition genügen:

- weniger als 250 Beschäftigte (Mitarbeiterzahl / Jahresarbeitseinheit JAE)
- Jahresumsatz von weniger als 50 Mio. € oder Jahresbilanzsumme von weniger als 43 Mio. €.

Bei der Berechnung der Mitarbeiterzahl und des Jahresumsatzes bzw. der -bilanzsumme werden Kapital- oder Stimmrechte an und von anderen Unternehmen berücksichtigt, indem bei der Klärung des KMU-Status die Mitarbeiterzahl und die Finanzangaben dieser anderen Unternehmen anteilmäßig zu den eigenen Daten addiert werden. Informationen zur Vorgehensweise finden Sie im Benutzerhandbuch der Europäischen Kommission zur KMU Definition:

[http://ec.europa.eu/enterprise/enterprise\\_policy/sme\\_definition/sme\\_user\\_guide\\_de.pdf](http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide_de.pdf)

### **Evaluierungskriterien**

In Annex 2 des „Guide for Applicants“ erhalten Sie einen Einblick in die Evaluierungskriterien. Vorgehen sind die Kriterien:

- S/T Quality: Wissenschaftlich-technologische Exzellenz in Bezug zu den ausgeschriebenen Topics
- Implementation: Qualität und Effizienz der Projektimplementierung und des Managements
- Impact: Potenzielle Auswirkung durch Entwicklung, Verbreitung und Nutzung

Für jedes dieser Kriterien werden durch unabhängige Gutachter maximal 5 Punkte, das heißt, insgesamt 15 Punkte vergeben. Um als förderwürdig eingestuft zu werden, müssen pro Kriterium minimal 3 Punkte, insgesamt jedoch mindestens 10 Punkte erreicht werden. Falls das Budget nicht die Förderung aller als förderwürdig eingestuften Vorschläge zulässt (Regelfall), erfolgt die Auswahl der zu fördernden Projekte anhand eines Rankings auf Basis der erreichten Gesamtpunktzahl.

## Partnersuche

Die Gewinnung von Partnern ist eine der großen Herausforderungen in der Antragstellung. Das Team der Nationalen Kontaktstelle Sicherheitsforschung unterstützt Sie gern bei der Suche nach europäischen Projektpartnern. Die Kontaktdaten des Teams finden Sie am Ende dieses Informationsbriefes.

### Partnering Platform der Nationalen Kontaktstelle Sicherheitsforschung

Neben der persönlichen Unterstützung stellt Ihnen die Nationale Kontaktstelle eine Partnering Platform als ein weiteres Instrument für die Partnergewinnung zur Verfügung.

Auf der Partnering Platform können Sie nicht nur Ihre **Projektideen bewerben** oder Ihre **Kompetenzen veröffentlichen**, sondern auch **in bestehenden Profilen suchen**. Dabei erlaubt es die Plattform, Einträge spezifischen Topics des jeweils ausgeschriebenen Sicherheitsforschungs-Arbeitsprogramms zuzuordnen. Interessierte Teilnehmerinnen und Teilnehmer können damit sowohl nach bestimmten Schlüsselwörtern als auch gezielt nach einzelnen Topics suchen. Weiterhin prüft die Nationale Kontaktstelle sämtliche Einträge der Datenbank auf Plausibilität, um eine hohe Qualität und Aktualität der Partnerprofile zu gewährleisten.

Die Plattform ist für alle interessierten Akteure unabhängig vom Herkunftsland geöffnet. Für die Nutzung der Partnering Platform werden **keine Gebühren** erhoben. Die Plattform wird von der Nationalen Kontaktstelle Sicherheitsforschung und damit wettbewerbsneutral betrieben.

Um Partnergesuche aufzugeben oder nach Partnern zu suchen, können Sie die Partnering Platform **ab dem 25. Juli 2011** unter folgender Adresse erreichen:

<http://www.partnering-platform.com/>

### FP7 Security Research Info Day & Partnering Event

Am 8. September 2011 findet der FP7 Security Research Info Day in Brüssel statt. Auf diesem Informationstag können Sie nähere Informationen zum Arbeitsprogramm des 5. Calls erhalten. Darüber hinaus bietet die Veranstaltung, auf der auch ein Partnering Event stattfinden wird, einen guten Rahmen, um neue Projektpartner zu finden und Fragen zum Inhalt und den formalen Bedingungen des Calls zu klären.

Weitere Informationen und Online-Anmeldung:

[http://ec.europa.eu/research/rea/index.cfm?pg=security7fp\\_infoday2011](http://ec.europa.eu/research/rea/index.cfm?pg=security7fp_infoday2011)

### **Brokerage/Partnering Event auf der SRC'11**

Am 19. September 2011 findet auf der SRC'11 (Warschau) ein Brokerage/Partnering Event zum 5. Call des europäischen Sicherheitsforschungsprogramms statt. Während dieser Veranstaltung haben Sie die Gelegenheit, Gespräche mit möglichen Projektpartnern zu führen.

Weitere Informationen und Online-Anmeldung:

[http://www.src11.eu/strona/69/19\\_september\\_brokerage\\_event.html](http://www.src11.eu/strona/69/19_september_brokerage_event.html)

Eine Möglichkeit zur Registrierung für den Brokerage Event besteht bislang nicht. Sobald dies der Fall ist, werden wir entsprechende Informationen auf der Webseite der Nationalen Kontaktstelle Sicherheitsforschung veröffentlichen.

### **Aufruf zur Eintragung als Gutachter**

Die Evaluierung der im Forschungsrahmenprogramm eingereichten Projektanträge erfolgt durch unabhängige Gutachter. Die Europäische Kommission wählt hierzu für jeden Call die Gutachter entsprechend ihrer Expertise aus einer Datenbank aus. Wir möchten Ihnen die Teilnahme als Gutachter empfehlen. Bisherige Gutachter berichten, dass die während der Evaluation gewonnene Erfahrung sehr hilfreich auch für die Vorbereitung von künftigen Anträgen ist.

Sie können sich selbstständig in die Gutachter-Datenbank eintragen. Bitte beachten Sie, dass Ihre Chancen, ausgewählt zu werden, steigen, wenn Sie die Schnittmenge Ihrer Expertise mit den Themen des aktuellen Calls identifizieren und die entsprechenden Kernbegriffe in Ihrer Datenbankeintragung benennen. Die Gutachtertätigkeit wird finanziell vergütet.

Weitere Informationen und Online-Anmeldung unter:

<https://cordis.europa.eu/emmf7/>

### **Ansprechpartner in der Nationalen Kontaktstelle Sicherheitsforschung**

Folgende Mitarbeiter stehen Ihnen beratend und unterstützend bei der Vorbereitung von EU-Anträgen zur Verfügung:

Dr. Thorsten Fischer

Fon: + 49 (0) 211 62 14 - 628

Fax: + 49 (0) 211 62 14 - 484

E-Mail: [fischer\\_t@vdi.de](mailto:fischer_t@vdi.de)

Dr. Steffen Muhle

Fon: + 49 (0) 211 62 14 – 375

Fax: + 49 (0) 211 62 14 – 484

E-Mail: [muhle@vdi.de](mailto:muhle@vdi.de)

Hinweis gemäß § 33 des BDSG: Der Versand des Informationsbriefes erfolgt über eine Adressdatei, die mit Hilfe der automatisierten Datenverarbeitung geführt wird.

Falls Sie den Informationsbrief zur Sicherheitsforschung in Zukunft nicht mehr erhalten wollen, klicken Sie bitte [hier](#).

Wir freuen uns, wenn Sie diesen Informationsbrief an interessierte Kollegen oder Partner weiterleiten. Falls Sie diese Mail weitergeleitet bekommen haben und auch in Zukunft über Neuigkeiten zur Sicherheitsforschung (Förderbekanntmachungen, Veranstaltungshinweise, etc.) informiert werden wollen, können Sie den Informationsbrief zur Sicherheitsforschung [hier](#) abonnieren.

Mit freundlichen Grüßen

Projektträger Sicherheitsforschung

Dr. Andreas Hoffknecht

Fon: + 49 (0) 211 62 14 - 456

Fax: + 49 (0) 211 62 14 - 139

E-Mail: [hoffknecht@vdi.de](mailto:hoffknecht@vdi.de)

Dr. Thorsten Fischer

Fon: + 49 (0) 211 62 14 – 628

Fax: + 49 (0) 211 62 14 – 484

E-Mail: [fischer\\_t@vdi.de](mailto:fischer_t@vdi.de)

VDI Technologiezentrum GmbH

VDI-Platz 1

D-40468 Düsseldorf



PROJEKTTRÄGER FÜR DAS



# Anhang

## 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 <sup>1</sup>
- **Indicative budget:** Total call budget EUR 241.7 million <sup>2</sup>

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 |
|---|--|-----------------|
| <b>Activity: 10.1 Increasing the Security of the Citizens</b> |  |                 |
| 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           |

<sup>1</sup> The Director-General responsible may delay this deadline by up to two months.

<sup>2</sup> 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        |
| <b>Activity: 10.2 Security of infrastructures and utilities</b>    |  |              |
| 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        |
| <b>Activity: 10.3 Intelligent surveillance and border security</b> |  |              |
| 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 |
| <b>Activity: 10.4 Restoring security and safety in case of crisis</b> |  |       |
| 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                                    |
| <b>Activity: 10.5 Security systems integration, interconnectivity and interoperability</b> |  |  |
| 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   |  |
| <b>Activity: 10.6 Security and society</b>   |  |  |
| 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 |
| <b>Activity: 10.7 Security Research coordination and structuring</b>     |  |           |
| 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:

| <b>Funding scheme</b>  | <b>Minimum conditions</b>  |
|------------------------|--|
| 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](http://cordis.europa.eu/fp7/find-doc_en.html) under 'Guidance documents/Flat rates for daily allowances'.