***WORK PROGRAMME 2012***

# *COOPERATION*

## THEME 10

### *SECURITY*

*(European Commission C(2011)5068 of 19 July 2011)*

*Table of content*

**Objective:**

The objective of the Security theme is to develop the technologies and knowledge for building capabilities needed to:

- ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental rights including privacy,
- ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security,
- stimulate the cooperation of providers and users for civil security solutions,
- improve the competitiveness of the European security industry and
- deliver mission-oriented research results to reduce security gaps.

# I CONTEXT

A secure Europe is the basis for planning our lives, for economic investments, for prosperity and freedom. The Security theme contributes to the implementation of EU external policies[1], to the creation of an EU-wide area of freedom, justice and security[2], in the context of the "Stockholm Programme", and to policy areas such as transport[3], health[4], civil protection[5], energy,[6] development[7] and environment[8].

Through this, the Security theme also contributes to the *Europe 2020* strategy[9] and its *Innovation Union* flagship initiative[10], by promoting growth and employment in general, stimulating innovation (including in SMEs), enhancing the competitiveness of European industry, closing the gap between research and market, ensuring a better involvement of SME's, and responding more rapidly to current needs and enhancing international cooperation.

The Innovation Union initiative underlines that research and innovation are key drivers of competitiveness, jobs, sustainable growth and social progress. The work programme 2012 has been designed to support the implementation of the Innovation Union Initiative and in particular to bring together research and innovation to address major challenges.

This work programme contributes to the innovation objective in particular by supporting more topics aimed at generating knowledge to deliver new and more innovative products, processes and services. For this reason the possibility of submitting proposals that include significant testing, validation and demonstration activities in response to all topics (i.e. not only within the already existing "demonstration programmes") has been included, as well as a topic on pre-operational validation.

---

1 http://www.eeas.europa.eu/index_en.htm
2 http://ec.europa.eu/dgs/home-affairs/index_en.htm
3 http://ec.europa.eu/transport/index_en.htm
4 http://ec.europa.eu/health/index_en.htmv
5 http://ec.europa.eu/echo/civil_protection/civil/index.htm
6 http://ec.europa.eu/dgs/energy/index_en.htm
7 http://europa.eu/pol/dev/
8 http://ec.europa.eu/dgs/environment/index_en.htm and http://ec.europa.eu/clima/news/index_en.htm
9 COM(2010) 2020
10 COM(2010) 546

This work programme is also contributing to the innovation union by identifying and addressing exploitation issues, like capabilities for innovation and dissemination, and by enhancing the use of the generated knowledge (protection of intellectual property rights like patenting, preparing standards, etc).

Information on the Risk-Sharing Finance Facility (RSFF), an innovative financial instrument under FP7, is available on line[11]. The Commission will respond to further needs of potential beneficiaries for information on the RSFF (by, e.g., awareness-raising activities in conjunction with the European Investment Bank, participation to thematic events).

The respect of privacy and civil liberties is a guiding principle throughout the theme. All individual projects must meet the requirements of fundamental rights, including the protection of personal data, and comply with EU law in that regard.

The Security theme has an exclusively civil application focus.

The Security theme facilitates the various national and international actors to co-operate and coordinate in order to avoid unnecessary duplication and to explore synergies wherever possible. Furthermore, the Commission will ensure full complementarity with other EU initiatives and avoid duplication, e.g. with the 'Framework Programme on Security and Safeguarding Liberties' (SSL), which focuses on actions related to policy and operational work in the area of law enforcement and combating and preventing crime/terrorism, while the Security theme supports R&D actions oriented towards new methodologies and technologies.

Following the recommendations of the Commission's *European Security Research Advisory Board (**ESRAB**)*[12] in September 2006, the Security theme addresses four security **mission areas** of high political relevance which relate to specific security **threats**. It contributes to building up the necessary **capabilities** for safeguarding security in these mission areas by funding the research that will deliver the required **technologies and knowledge** to build up these capabilities.

It is clear moreover, that the use of security related technologies must always be embedded in political action. To support this and also to improve the effectiveness and efficiency of the technology related research, three areas of **cross-cutting** interest are selected as well.

In September 2007, the *European Security Research and Innovation Forum (**ESRIF**)* was established with 64 high level members, including two representatives of the European Commission, and over 600 experts. The objective of ESRIF was to develop a mid and long term Joint Security Research Agenda that will link security research with security policy making and its implementation. The ESRIF Final Report[13] was published in December 2009. In its communication responding to the ESRIF Report[14], the Commission welcomed it and acknowledged its importance in the context of the FP7 Security theme.

The overall structure of the Security theme, including the seven activity areas, is summarised in the following table:

[11] http://www.eib.org/products/loans/special/rsff/?lang=en

[12] *ESRAB Report: Meeting the Challenge: the European Security Research Agenda - A report from the European Security Research Advisory Board, September 2006. ISBN 92-79-01709-8.*

[13] See www.esrif.eu

[14] COM(2009)691

**Security mission areas:**

1. Security of citizens
2. Security of infrastructures and utilities
3. Intelligent surveillance and border security
4. Restoring security and safety in case of crisis

**Cross-cutting areas:**

5. Security systems integration, interconnectivity and interoperability
6. Security and society
7. Security Research coordination and structuring

The Security theme aims at **meeting its main objectives – improved security for the citizens,** and **enhanced competitiveness for industry.** Successful demonstration of the appropriateness and performance of novel solutions is a key factor for the take-up of the output of the research work and its implementation by security policies and measures. The Security theme should also support the (re)structuring of the European security sector.

Funding modalities

Research in the Security theme consists of several building blocks, representing three - in some cases parallel, in others subsequent - routes that contribute to the overall objectives (see figure 1):

- On the lowest level of the building block structure, '**Capability Projects' (CPs)** aim at building up and/or strengthening security capabilities required in the four security missions. This will be done through *adaptation of available technology* as well as the development of *security specific technology and knowledge aiming at tangible results.* In many cases these will also have cross-mission relevance.
  Typical duration: 2-4 years
  Funding scheme: *Collaborative Projects*

- On the medium level of the building block structure, '**Integration Projects' (IPs)** aim at mission specific combination of individual capabilities providing a security *system* and demonstrating its performance.
  Typical duration: 3-4 years
  Funding scheme: *Collaborative Projects*

- On the top level of the building block structure, '**Demonstration Programmes' (DPs)** will carry out research aiming at large scale integration, validation and demonstration of new security systems of systems going significantly beyond the state of art. They depend upon the compatible, complementary and interoperable development of requisite system and technology building blocks of the integration projects and capability projects. They intend to promote the application of an innovative security solution, which implies a strong involvement of end users, taking into account the relevant legal and society related issues, and strong links to new standardisation. ESRAB identified five topic areas for Demonstration programmes: 1) Aftermath crisis management, 2) Border control, 3) Logistic and supply chain security, 4) Security of mass transportation and 5) CBRNE. Demonstration programmes will be implemented in two phases:

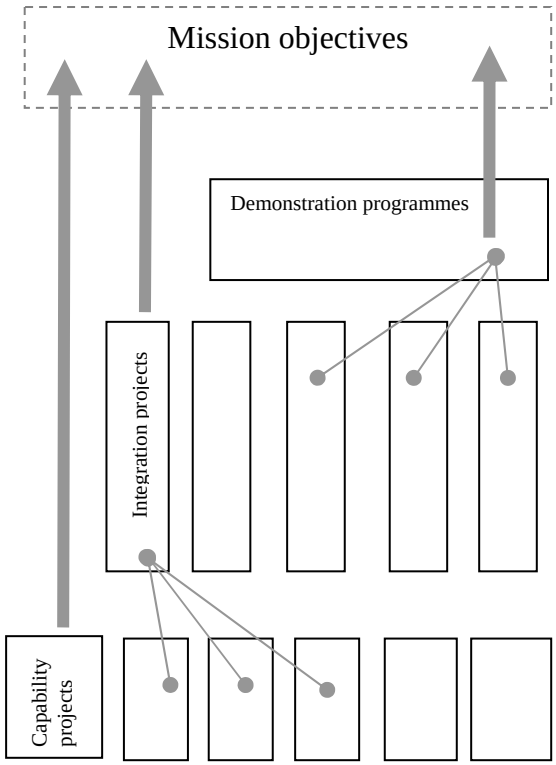



*Figure 1: Research routes to meet the Security theme objectives*

Phase I projects (either one or several projects in each of the demonstration programmes) will define the strategic roadmaps and trigger Europe wide awareness, both elements involving strategic public and private end users as well as industry and research. The strategic roadmaps will take into account relevant completed, ongoing and planned work and indicate further research needs for Security theme integration projects and capability projects, but also for other themes of the Seventh Framework Programme or for the national level.
Typical duration: 1 year
Funding scheme: *Coordination and Support Actions*

Phase II projects (either one or several projects in each of the demonstration programmes) will then technically implement the system of systems demonstration, taking already into account steps which have to follow the research, like certification and/or standardisation (if and as appropriate), development of marketable products and pre-procurement. This will mobilise a significant volume of resources.
Typical duration: 3- 4 years
Funding scheme: *Collaborative Projects*

- **Pre Operational Validation (POV)**: a new aspect for the theme in the Work Programme 2012 is the inclusion of a pilot funding of Pre Operational Validation. This funding modality would differ from and complement the other funding modalities such as CPs, IPs, DPs and also joint technology initiatives, etc., by involving directly – and supporting financially - end-user agencies (typically national or European authorities). This would

shorten time to market and encourage market acceptance of new technologies when seen as part of a coordinated policy framework, including: standardisation, certification and regulation of innovative goods and services (and eventually facilitating coordination of procurement policies). POV could either be via a decentralized network (of national agencies / public bodies) or via a single EU Agency, or both. The basic idea of a POV scheme is to support the *demand* side of research, rather than the *supply* side in their direct quest for new security solutions.

In this scheme, funding would be in general for one (or both) of two purposes:
(i) the *coordination* of relevant institutions or authorities (as appropriate), acting as *certifiers* of new technologies (100% support); and
(ii) the actual *implementation* of the corresponding calls for tenders (50% support[15]), for testing/validation of novel security solutions (implemented according to the own criteria and specifications of the participating institutions or authorities).
Typical duration: 3- 4 years
Funding scheme: a combination of *Coordination and Support Actions* (for coordination of validation policies) and *Collaborative Projects* (for implementation of testing and validation).

For the **cross-cutting domains** of the Security theme, actions can be both self standing or linked to the missions in activities 1 to 4. Society relevant research issues will also be, as far as possible, integrated in technology projects.

Funding schemes

In the general context of FP7 model grant agreements, the following funding schemes are envisaged:

- **Collaborative Projects** in this work programme are divided into
    a) small or medium-scale focused research project (CP-FP), and
    b) large scale integrating project (CP-IP).

*Demonstration Projects (Phase II) and Integration projects* described above will be implemented using the funding scheme Collaborative Project (large scale integrating project) with an indicative EU requested funding of over EUR 3 500 000.

*Capability projects* will be implemented using the funding scheme Collaborative Project (small or medium-scale focused research project) with an indicative requested funding of EUR 3 500 000 and below.

Within the above indicative funding levels, proposals should strive to be **as small and simple as possible** (e.g. avoiding unduly large and complex consortia) **and as large as necessary**. In other words, the size of projects – and of consortia – should be the result of, and justified by, the intended project objectives, and not the other way round!

- The **Networks of Excellence** (NoE) aims at research organisations, end users and other stakeholders that wish to combine and integrate in a durable way a large part of their activities

[15] In case of "Market Failure", funding of up to 75% of the related research activities can be envisaged, in analogy with the equivalent rule in Capability Projects (see also footnote 15).

and capacities in a given field, in a 'Joint Programme of Activities', possibly with a view of creating in this field a European 'virtual centre of research'.

The main purpose of this funding scheme, in the context of the Security theme, should be to promote new collaborative networks between research players with limited experience (e.g. end-users) or limited mutual knowledge (e.g. new research networks). The main emphasis, in this case is less on the achievement of specific pre-defined research results, and more on establishing a form of distributed centre of scientific and technological excellence, in line with the wider goals of the European Research Area.

- **Coordination and Support Actions** (CSA) are divided in Coordination Actions and Support Actions. Core activities will be studies, networking, exchanges of personnel, exchange and dissemination of good practices, the definition and organisation of joint or common initiatives, meetings, conferences and events etc. and the management of the action.

75% funding for research activities

In the Security theme (and *only* in this theme), the EU funding for research activities may reach a **maximum of 75%** in cases with very **limited market size** and **a risk of 'market failure'**, and for **accelerated equipment development** in response to new threats.[16] To claim this higher funding level, proposers need to demonstrate in their proposal that the required conditions apply. Please note that this higher funding level applies *only* to research activities, whereas demonstration activities are excluded from these provisions. Please note that these special provisions should not be confused with the 75% funding rate that is anyway available to SMEs all throughout FP7, independent of market conditions.

The forms of model grant agreements to be used for the funding schemes for the Security theme are outlined in Annex 3.

SME relevant research

All actions are open to the participation of all security stakeholders: industry, including Small and Medium Enterprises (SMEs), research organisations, universities, as well as public authorities, non-governmental organisations and public and private organisations in the security domain. Considering the Security theme's objective of increasing the competitiveness of industry, the broad **involvement of SMEs** in consortia is highly encouraged. The topics concerned by this specific action are explicitly mentioned in the description of the topics.

Moreover, in order to further promote the participation of SMEs in the Security theme, an **open topic for SMEs** has been included in part II of this Work Programme.

International Cooperation[17]

All actions of the Security theme are open to **international co-operation** to industrialised countries as well as to ICPC[18] countries. As a specific action, a number of topics are

[16] *Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013) Art 33.1*

[17] http://cordis.europa.eu/fp7/ict/international/st-agreements_en.html

[18] *ICPC: International Co-operation Partner Countries - see Annex 1.*

earmarked for an enhanced international cooperation, through a *recommended* participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities. The topics concerned by this specific action are explicitly mentioned in the description of the topics.

Dissemination actions

In general, particular networks of security research stakeholders (including both the supply and the demand side) are seen as instrumental in promoting the **dissemination** of security research to its end users, national public authorities and citizens alike. Attention is drawn to the exploitation strategy requirements, which is part of the evaluation criterion 3, Impact. Suitable and dedicated coordination and support actions to achieve this could also receive funding. It is important to strengthen these activities in all projects.

Further theme specific information

In order to ensure that the outcome of the research carried out under the Security theme does in particular contribute to meeting the theme's main objective - the improvement of the security of the citizens - co-operation between the user side (authorities and organisations responsible for the security of the citizens) and the supply side of security technologies and solutions must be promoted. Thus the active **involvement of end users** in the projects is considered of utmost importance. Whenever possible, this should translate into a direct participation of user organisations to the consortia implementing research actions (though other forms of indirect participation might also be followed, as appropriate).

Security theme actions should generally be **multidisciplinary** and **mission-oriented**. A multi-purpose nature of technologies is encouraged to maximise the scope for their application, and to foster cross-fertilisation and the actual take-up of **critical technologies** for the civil security sector.

The **testing**, **validation** and **demonstration** of the security solutions developed in the projects, involving as much as possible the end users, is considered at the core of the Security theme. These activities should be present in every type of project (as appropriate): *Demonstration Programmes* but also *Integration Projects* or *Capability Projects*. **Concrete achievements** and milestones are strongly encouraged, in particular in terms of expected impact.

Proposers are also encouraged to take into account **the pre-normative research dimension** in the Security theme. Research projects should focus, when possible, on the analysis and development of standards in the context of their research, thus supporting the creation of EU wide standards for security technologies.

Standards are considered crucial for interoperability and take up of research results. Preparation and promotion of standards within the projects is encouraged. Self-standing actions related to **interoperability and standardisation** are open in the Security call 5.

Attention must be given to the **societal impact** of the proposed solutions. Respect for fundamental rights and compliance with European societal values, including privacy issues, need to be embedded in each proposal and foreseen in the proposal's work plan. Proposals

should consider possible side effects of technological solutions to security problems and assess alternatives with the least intrusive effects on privacy and freedom. A holistic approach to security will take the perception of citizens into account and focus on dimensions such as perceived security, while being aware of the fact that security risks can be unevenly distributed within and between societies. Proposers are encouraged to develop solutions strengthening societal resilience and active participation of citizens as security enhancing resources.

Security research can also cover areas of (so called) '**dual use'** technology relevant to both civilian and defence applications. Appropriate coordination mechanisms are in place with the *European Defence Agency* (EDA), who will consult its Member States about national programmes, thus ensuring complementarity.

Actions within the Security theme build not only on technology gain from the capability projects, but also on research outcomes of other origins. Issues of **European added value** and large scale integration are covered in the theme, and complementarity is ensured with all other EU actions. Complementarity with research carried out in FP7 Associated Countries will be ensured via the members of the Security Programme Committee configuration.

**Gender aspects** in planning, decisions, and funding must always be taken into account, both as integrated research activities and as diversity in workforce. The pursuit of scientific knowledge and its technical application towards society requires the talent, perspectives and insight that can only be assured by increasing diversity in the research workforce. Furthermore sometimes security needs to be balanced against the accessibility needs of persons with disabilities. Therefore, a balanced representation of diverse branches of knowledge and of women and men as well as person with disabilities where relevant at all levels in research projects is encouraged, including in evaluation groups etc.

Security issues could also be regarded as intrinsic elements of **other themes in the Co-operation programme**. The scope of the calls has been carefully defined throughout the themes, in order to avoid gaps or duplication during the entire Seventh Framework Programme. Thus in case of doubt, whether a proposal is fully in scope with the topics presented under this theme, it is recommended to consult as well the Work Programmes of the other Co-operation themes.

Classified Information

Due to the sensitivity of the Security theme, the *Rules for participation*[19] of FP7 foresee the possibility of restrictions to the dissemination of the outcome of the actions on a case by case basis. In particular, special provisions for **classified information** will be taken in the grant agreement, as necessary and appropriate.

For the Security Research Call 5 (FP7-SEC-2012-1), **proposals must not contain any classified information**. This would lead to declaring them ineligible immediately. However, it is possible that the output of an action ('Foreground') needs to be classified, or that classified inputs ('Background') are required. In such cases proposers have to ensure and provide evidence of the adequate clearance of all relevant facilities. Consortia have to clarify

[19] *Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013) Article 22*

issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal. Proposals need to provide a draft *security classification guide*[20], indicating the expected levels of classification. Appropriate arrangements will have to be included in the consortium agreement.

Positively evaluated proposals involving sensitive or classified information, those involving international co-operation as well as those collaborative projects where 75% funding for research activities 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.

**Research Executive Agency**

Call for proposals under this work programme part (Security) will be implemented by the Research Executive Agency[21] (REA). The management of all projects to be funded as a result of this call for proposals will be implemented by REA, with the exception of:

- Classified grant agreements and contracts, and
- Policy related actions (explicitly indicated in section II of this work programme).

20 'Security Aspects Letter (SAL)': a set of special contractual conditions, issued by the contracting authority, which forms an integral part of a classified contract involving access to or generation of EU classified information, and that identifies the security requirements or those elements of the classified contract requiring security protection.

'Security Classification Guide (SCG)': a document which describes the elements of a programme, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, contract or grant agreement, and the elements of information may be re-classified or downgraded. The SCG must be part of the SAL.

See Commission Decision 2001/844/EC, ECSC, Euratom on security, amended by Decisions 2006/548/EC, Euratom and 2005/94/CE, Euratom.

21 See Commission decision C/2008/3980 of 31 July 2008 "delegating powers to the Research Executive Agency with a view to performance of tasks linked to implementation of specific EU programmes People, Capacities and Cooperation in the field of research comprising, in particular, implementation appropriations entered in the EU budget"

# II SECURITY RESEARCH CALL 5 (FP7-SEC-2012-1)

The primary ambition of the Security theme is to develop innovative security solutions and to facilitate their rapid take-up for the implementation of security policies and programmes.

All seven activity areas, the four mission-oriented and the three cross-cutting areas have topics in the Security call 5. Topics address one (or more) of the following four **ambitions**:

- important **capability gaps** (urgent needs that can easily be fulfilled with new solutions based on innovative technologies),
- **validation** of solutions resulting from research and development (experimentation involving their appropriation by the end-users),
- core **critical capabilities** needed by Europe (where technologies are not yet mature),
- **high risk / high pay-off** projects (with a view at long-term development of groundbreaking new technologies).

The topics that are open to the submission of proposals under the Security Research Call 5 are described in the following seven sections corresponding to the seven activity areas. For each area, the description is taken from the FP7 Cooperation Specific Programme. Then, topics are presented within each area. Proposers are expected to cover the topic in its entirety unless otherwise specified in the description of the topic in question.

## *Activity: 10.1 Increasing the Security of the Citizens*

Actions in this activity will concentrate on threat aspects of potential incidents of a trans-national importance, such as offenders, equipment and resources used by them or as mechanisms of attack. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases 'identify', 'prevent' and 'prepare' and 'respond'. The ambition is both to avoid an incident and to mitigate its potential consequences. To build up the required capabilities with the aim of providing civil protection, including bio-security and protection against risks arising from crime and terrorist attacks, emphasis will be on issues such as: threat (e.g. Chemical, Biological, Radiological and Nuclear, CBRN) awareness (e.g. intelligence gathering, collection, exploitation, sharing; alerting), detection (e.g. hazardous substances, explosives, agents B or C, individuals or groups, suspect behaviour), identification and authentification (e.g. of persons, type and amount of substances), prevention (e.g. control of access and movements, with respect to financial resources, control of financial structures), preparedness (e.g. risk assessment; CBRN protection, control of intentionally released biological and chemical agents; assessment of levels for strategic reserves such as manpower, skills, equipment, consumables; with respect to large scale events, etc.), neutralisation (e.g. missiles, communications, vehicles, non-destructive systems) and containment of effects of terrorist attacks and crime, law enforcement data processing.[22]

[22] The definitions of the Activities presented in the "boxes" are directly referring to the Specific Programme for the FP7 security Theme, see page 135:

This activity is divided among five areas: **Organised crime; Intelligence against terrorism; Explosives; Ordinary crime and Forensic; CBRN Protection and information gathering**. It should be noted that the intelligence against terrorist activities is mainstreamed across many other areas.

***Area: 10.1.1 Organised crime***

No specific topic for this area has been planned for this call.

***Area: 10.1.2 Intelligence against terrorism***

No specific topic for this area has been planned for this call.

***Area: 10.1.3 Explosives***

### *Topic SEC-2012.1.3-1 Less than Lethal Handling of PBIEDs - Capability Project*

**Description of topic:**
Suicide bombing has been seen in a number of EU Member States/Associated Countries, and could occur in any Member State/Associated Countries. This research should identify means of dealing with that threat.

The task is to determine ethical and socially acceptable technical measures to deal with a person suspected of carrying a person-borne improvised explosive device (PBIED) when close to the intended time and point of attack, balancing safety to the public, safety of first responders and security personnel, and the rights of the individual.

Research must consider and develop measures to contain/minimise the potential injuries and fatalities, prevent the suspected bomber from triggering the device, prevent the device from activating or being activated, and removing the threat without resorting to use of lethal force.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Limit the attractiveness of suicide attacks and increase the security of European citizens and security forces.

### *Topic SEC-2012.1.3-2 Home made explosives (HMEs) and recipes characterisation - Capability Project*

**Description of topic:**
The objective is to establish basic knowledge hitherto unknown about HMEs; their composition and characterisation. The task is also to review freely available recipes (for instance on Internet) and to evaluate their dangerousness.

---

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:400:0086:0242:EN:PDF

During the study, several basic questions should be answered:
- How can HMEs be produced from ordinary commercially available chemicals and materials?
- What type of chemicals are available freely today for the direct use in HMEs?
- How can freely available chemicals be easily chemically changed or concentrated so that they can be used for the production of HMEs?
- What are the concentration limits of precursors or HME formulations for them to be usable by terrorists?
- What is the chemical stability of HME? (What time span does a terrorist have between the production of an HME and the execution of an attack?)
- What can be done to prevent or inhibit the production of HMEs?

The research of this project must be performed in close collaboration with manufacturers of precursors. This project also requires the participation from end users such as police or security forces. Extensive attention should be given to dual-use and ethical issues.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** To increase the security of European citizens and polices forces through a better knowledge of HMEs; to reduce the possible occurrence of events using HME; to help the detection of bomb factories with a better knowledge of the chemicals involved.

### ***Area: 10.1.4 Ordinary Crime and Forensic***

No specific topic for this area has been planned for this call.

### ***Area: 10.1.5 CBRNE Protection***

## *Topic SEC-2012.1.5-1 CBRNE Demo Phase II*[23]

**Description of topic:**
Accidental or deliberate CBRNE events are widely considered as low probability events that might however have a big impact on the citizens and the society. Whenever and wherever they happen, they usually deserve a gradual (regional, national, European) and multi-facetted approach as they tend to provoke severe and unexpected physical, psychological, societal, economical and political effects that might also easily cross the borders inside as well as outside the EU.

Successful **CBRNE resilience** of the society require therefore a similarly multi-facetted system-of-systems approach, covering most of identified hazards and all effect levels along the whole CBRNE security cycle (threat assessment, prevention, preparedness, detection, response, recovery). This approach involves many relevant stakeholders. Among them, first responders (e.g. fire brigade, health services, police, operators…) and their competent national authorities are expected to be the main ***end-users***.

[23] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.

Proposals should take into account as much as possible relevant, existing, past or ongoing projects (for example earlier phase I projects on the same subject). This large demo phase II will cover the whole cycle of CBRNE aiming at developing and ensuring the resilience capacity of the EU society.[24] All demonstration efforts will be aimed at both integrating and coordinating existing EU capacities and competences.

This demo should develop a "**system of systems**" that will provide EU-tailored solutions able to improve CBRNE resilience and allow enhanced interoperability between CBRNE operators. The coherent ensemble of demonstrations should cover at least multiple hazards (C, B, R, N, E), multiple phases of the security cycle (prevention to recovery), multiple tiers of effect (regional, national, European) and multiple stakeholders (end-users in particular first responders, authorities, industry, R&T platforms). Preferably, demonstrations should take place in a (semi-)operational context, including testing and validation, as well as simulation if required.

The institutional end users are those in the best position to define and assess the performances of the future system of systems to be demonstrated, particularly in terms of capabilities to provide improved security solutions. These should be experimented in a pre-operational scenario, to be defined by representatives of institutional users belonging to different MS.

**Possible locations for demonstrations activities:**
The different CBRNE demonstrators and procedures will be tested in selected cities and/or locations and/or sensitive infrastructures of the European Union, considered of high relevance, such as open places (city main squares, touristic spots, border checks, cross border rivers...) or confined infrastructure like transports hubs, large stadium, theatres, food or water supplies. Due to the sensitivity and scale of CBRNE live or real time demonstrations, a careful attention will be paid to their preparation, organisation and communication to the public, involving local and/or national and/or EU authorities wherever and whenever necessary.

**Links with other CBRNE activities:**
Given the cross-cutting character of CBRNE, linkages with other ongoing or completed Research activities and studies (across all FP7 Themes and other national or European funding schemes, Instrument for Stability, European Framework Cooperation, etc.) should be carefully considered to ensure complementarities, integration and avoid duplications.

Indeed, no single technological solution exists with the capability to meet the variety of operational requirements. No equipment and information system in operation or under deployment (even for defence needs) is currently able to respond to all the above requirements. However, **in a few years from now**, significant technical and knowledge progress is expected from all ongoing security projects, (national R&D programs, FP7, EDA,…) combining for example different sets of CBRNE sensors and platforms, heterogeneous data processing and fusion, communication and crisis management tools, new methodologies for protecting first responders and advanced forensic protocols. They should therefore be usefully integrated to build up an innovative EU CBRNE system for national, regional and European missions to efficiently provide CBRNE applications in public area as well as critical infrastructure.

[24] Further guidelines and relevant policy background in the area of CBRN can be obtained from the dedicated Security Research web-site of EUROPA (http://ec.europa.eu/enterprise/security/index_en.htm).

Ultimately, any demonstration proposal should clearly identify and demonstrate the real EU added value of each CBRNE demonstration compared to existing capabilities, competences and systems. A key accent will be put on cross border cooperation, interoperability, standardisation and certification, EU-coordination and communication. The proposal should have a clear eye for inclusion of multi-usability of CBRNE capabilities to make them affordable. An appropriate balance between R&D investment, expected market benefits and impacts on the EU society should be reached.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** Solutions will demonstrate the added value of large scale integration of CBRNE counterterrorism improving effectiveness, efficiency, coherence, and cooperation/coordination at the national and European level. Member States and their response organizations will be better equipped by improved integration and information sharing in countering the CBRNE threat. As a result EU society will be more resilient to the CBRNE threat.
In particular, this could be reflected qualitatively and quantitatively, for example, through the following non exclusive achievements:

- Shortening time to response (after an event occurs)
- Improving mass gathering/events security
- Enhancing the protection of sensitive or critical infrastructures
- Achieving a European lead in CBRNE sampling, detection, proficiency testing and forensics
- Boosting the EU civilian CBRNE market
- Reinforcing technological, societal and psychological resilience of the EU society

### *Topic SEC-2012.1.5-2 Improving drinking water security management and mitigation in large municipalities against major deliberate, accidental or natural CBRN-related contaminations - Capability Project*

**Description of topic:**
The main purpose is to create a platform for drinking water security against deliberate or accidental Chemical, Biological, Radiological or Nuclear ("CBRN": all of them or alternatively one or a combination of them) threats in major municipalities. It will cover development, assessment, demonstration, deployment, monitoring, and integration of innovative technology solutions in improving current practice of water security management.

The platform will focus on developing an integrated CBRN-control, on-site monitoring and decision support system that incorporates the use of innovative, affordable sensors for the detection of CBRN-contaminants in water supply systems. Designed for daily, on-site use by both water utilities and government/military organisations, products will provide water supply managers with reliable tools to efficiently support:

i) integration of innovative CBRN-sensors in intelligent monitoring systems;
ii) identifying bio-contamination risks and system vulnerabilities;
iii) classifying the severity of the -contamination event;
iv) evaluating the consequences and the propagation rate of the contaminated zones; and
v) identifying the most effective response and mitigation measures.

Today's laboratory-based contaminant testing systems coupled with the current practice of the use of contingency plans are impractical for daily monitoring usage. They operate too slowly for incident control and prevention since the full extent of the event can be rarely determined timely for efficient mitigation measures. The system should be designed to efficiently support i) on-site detection of the radiological, chemical and biological contamination event; ii) classification of its severity as -"green light", "yellow light", or "red light" and its nature; iii) assessment and display of the spatial and temporal propagation of consequences and risk zoning; iv) real-time intra-agency and inter-agency information sharing for situation analysis and response management; v) communication with stakeholders, media, and customers; and vi) identification and impact monitoring of mitigation measures.

This project will focus on technology assessment, demonstration, and capacity building for integrating innovative solutions in improving the current state of practice. Based on existing local, national and EU or international private and public structures and initiatives, this project will include relevant stakeholders as for example, where justified and appropriate, water utilities, bottled water and food industries

Given the cross-cutting character of CBRN threats, linkages with other ongoing or completed Research activities and studies (across all FP7 Themes and other national or European funding schemes, etc.) should be carefully considered to ensure complementarities, integration and avoid duplications

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** This platform will contribute to coordinate, integrate and improve the drinking water security management and mitigation in large cities at the EU and possibly international level.

### *Topic SEC-2012.1.5-3 Identification and development of low-risk alternatives to high-risk chemicals - Capability Project or Coordination and Support Action*

**Description of topic:**
As underlined in the EU CBRN action plan, high-risk chemicals can be used by malevolent individuals or organisations and are a security threat for civilian population. The research should look into the chemical or physical-chemical properties of high-risk chemicals, their ways of production, processing, transport and storage, and explore alternatives for lower risk chemicals. As a first step an inventory of substances in question is required. To this end, generic criteria should be defined, which cover all relevant aspects of the actual replacement process.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action (coordination action)

**Expected impact:** The scientific knowledge basis developed during the project should contribute to the reduction of production and use of high risk chemicals at mid or long term.

### *Topic SEC-2012.1.5-4 Securing the food chains from primary production and animal feeds to consumer ready food against major deliberate, accidental or natural CBRN contamination - Capability Project*

**Description of topic:**
Appropriate detection and management of any major deliberate, accidental or natural Chemical, Biological, Radiological or Nuclear ("CBRN") contamination make the free circulation of agrarian products (agricultural and ranching) and food in the single market more resilient. This project will draw up an exhaustive inventory of available and expected future diagnostic methods that could be potentially used for early detection (also at farm/on-site) of animal diseases or of contaminations (including industrial chemicals) throughout the food supply chain, modelling and prevention of spread; it will define the criteria for use and interpretation in a crisis context including alerting and reporting mechanisms and counter-measures; it will propose complementary means for high throughput screening and analysis (detection and identification) of multiple agents; it will also address sampling methods and sampling automation possibilities, including the reduction of false positives; the development of rapid on site (e.g. on farm; border post) tests for targeted CBRN agents, industrial chemicals and animal diseases should be considered. Technical and (inter-)organizational measures should be integrated and positive collateral effects on free movement of animals and food products as well as the quality of food should be considered.

The added value of such tools in the context of the EU policy should be carefully examined, including the synergy generated by these tools within the context of other similar EU initiatives currently funded in this area and for which other Commission DGs, Services and EU Bodies are responsible.

Given the cross-cutting character of CBRN contaminations, linkages with other ongoing or completed research activities and studies (across all FP7 Themes and other national or European funding schemes, etc.) should be carefully considered to ensure complementarities, integration and avoid duplications.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** To improve food security against any major deliberate, accidental or natural CBRN contamination. To reduce incidents with cross-border economic impacts and human casualties along European food supply chains. The EU level of expertise in this field should be significantly increased.

***Area: 10.1.6 Information Gathering***

### *Topic SEC-2012.1.6-1 Digital, miniaturised, operational tool for investigation - Capability Project*

**Description of topic:**
Investigations on the activities of criminal organizations (related with drugs or human trafficking, terrorism, or any other forms of organized crime) usually require Law Enforcement Agencies (LEAs) to use electronic equipment for legal recording, retrieving and

monitoring of criminal activities in a safe and unnoticed way, while keeping for both the sensors part and the monitoring station all the legal, integrity and chain-of-custody requirements that will enable the presentation of evidences obtained this way at the Courts of Justice.

Requirements for these equipments are very different from those offered by available commercial devices. Depending on the operation, the periods of time that these electronic devices have to work can range from days to months or in real time. Access to the device could be limited or impossible. Secure remote operation over radio channel (or other type of communication channel) should be possible. Other requirement may apply like small size for easy concealment, low power consumption for extended time life, robustness and self-protection in addition to strong authentication mechanisms for operators and protection of the communication channels.

The task is to develop new type of sensors, monitoring station and their associated communication channel for LEA operation on the field according to their specification and subject to their validation at the end of the project taking into account the societal acceptance of the proposed solutions.

Proposers for this topic should look for an enhanced SME participation as described in Part I of the Work Programme.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** This action is directed to the substantial improvement of existing technologies and the development of new ones, and their direct and practical application to day-to-day needs that Law Enforcement Agencies are not able to realize efficiently with available commercial products including testing, validation and demonstration as justified. Participation of LEAs in the definition of requirements and validation of results is essential, as only end-users are familiar with the challenges they frequently have to face in real operations within criminal investigations.

## *Activity: 10.2 Increasing the Security of infrastructures and utilities*

Actions in this activity will concentrate on targets of an incident or disaster of transnational importance, examples for infrastructures include large scale event sites, significant sites of political (e.g. parliament buildings) or symbolic (e.g. particular monuments) value and utilities being those for energy (including oil, electricity, gas), water, transport (including air, sea, land), communication (including broadcasting), financial, administrative, public health, etc. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases ‘protect’ but also ‘prepare’. The ambition is both to avoid an incident and to mitigate its potential consequences. To build up the required capabilities, emphasis will be on issues such as: analysing, modelling and assessing vulnerabilities of physical infrastructure and its operations; securing existing and future public and private critical networked infrastructures, systems and services with respect to their physical, logical and functional side; control and alert systems to allow for quick response in case of an incident; protection against cascading effects of an incident, defining and designing criteria to build new secure infrastructures and utilities.

This activity is divided among five areas: **Design, planning of buildings and urban areas; Energy, Transport, communication grids; Surveillance; Supply chain; and Cyber crime.**

The focus in the Cyber Crime area lies on the sets of tools, instruments, rules, etc. used for the prevention, detection, counteracting or investigation of, criminal (including terrorist) activities targeted to the cyber environment, in particular in connection with material or immaterial critical assets or infrastructures, and delivered through the cyber environment. As this area takes a threat and incident related approach only, it is complementary to the more general approach of the ICT Theme of the Cooperation Programme.

***Area: 10.2.1 Design, planning of buildings and urban areas***

## *Topic SEC-2012.2.1-1 Resilience of large scale urban built infrastructure - Capability Project*

**Description of topic:**
The task is to develop a concept to improve the security and resilience of large-scale urban developments. This topic focuses on large-scale buildings/building complexes/building arrangements such as shopping centres/areas, sports venues or combinations of business centres with underground transportation nodes. Security and resilience against disasters should be included at the design and planning phase of such projects, leading to robust built infrastructure invulnerable to natural and man-made disasters. The project will take into account the state of the art of built infrastructure protection products as well as planning and engineering tools.

Moreover, the above described urban built infrastructures represent a critical node within the intertwined networks of an urban area. Despite the fact that a substantial part of our critical infrastructures today rely on complex systems of communication networks, there is just as much of a need to take into account the equally vulnerable built infrastructures of modern urban areas. Many of these, be it transport systems of different kinds, large sports arenas or shopping malls have already been evaluated regarding their resilience against major terrorist attacks or disruptions of other natures. However, a comprehensive approach to develop resilience concept for a combination of such systems, as they are often designed in modern urban areas, should be taken into account.

Making large-scale built infrastructure in urban areas more resilient against attacks and disruptions of different kinds is an endeavour that requires multifaceted and multifunctional cooperation between various players of the security sector. In this case, resilience not only includes concepts and technologies to make built infrastructure more robust against attack and disruption, but also to integrate aspects such as energy efficiency, multi-functionality and overall sustainability of large-scale infrastructure. Moreover, sensor technologies could be used to guarantee the integrity of the build environment. The European construction industry (including civil engineering, architectural designs as well as building/construction) is already a strong player on the global market. Globally significant building projects of massive impact (Dubai, Shanghai, etc.) are often realized by European designers/builders. This strong position must be invigorated by the initiation of an integrated approach to better protect large-scale built infrastructure. Obviously, such an effort offers a wide range of new market opportunities for a wide range of European players. Evidently, this not only includes players developing genuine security technologies, but also requires smart and unconventional business solutions

to bring together the different aspects addressed by the concept of resilience. This will ensure that aside from the already established players on the field, new and young SMEs can contribute to such an approach with their niche ideas and concepts. Proposals should take into account as much as possible relevant, existing, past or ongoing projects.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** It is expected that action under this topic will improve the design of urban area and thus increase their security against and resilience to new threats. It is expected that it will lead to a systematic approach to resilience enhancements for large urban built infrastructures beginning at the design stage.

### *Topic SEC-2012.2.1-2 Criticality analysis and simulation, if appropriate, of critical infrastructure including concepts for forgery proof and efficient facility access systems - Capability Project*

**Description of topic:**
A better understanding of interdependencies within critical infrastructure sectors is necessary in order to define measures to achieve better resilience against threats to critical infrastructures and government buildings. In this connection new technological developments in the fields of surveillance as well as (physical) access techniques to critical infrastructures and government buildings should be explored. The analysis of criticality should therefore not only focus on potential threats caused by attacks or accidents, but also on the expected developments in these areas and the impacts and potential challenges of new technologies. Respective questions necessary to assure the societal acceptance of solutions produced by the project should be implemented accordingly.

Some dedicated government buildings are crucial in cases of crises and therefore also represent a kind of infrastructure hub in crisis situations i.e. for maintaining the day to day operational management of the country in question. Critical Infrastructure hubs and dedicated government buildings need to be safe and secure, minimising the risk of being put out of action by the crises/incidents. A higher resilience will enhance the restoration to a normal situation after the crisis/incident.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Development of a system to evaluate these hubs, dependencies and provide reliable tools for forecasting developments in technology and its use or application as well as human related factors. The development and test of simulation models for interdependences between critical infrastructures should in particular allow the estimation of vulnerabilities of interconnected infrastructures. Solutions for secure and quick physical access to CI key systems could be explored and tested in practise.

***Area: 10.2.2 Energy, Transport, communication grids***

### *Topic SEC-2012.2.2-1 Identification of measures to counter illegal export of metal-bearing waste - Coordination and Support Action*

**Description of topic:**
The aim of this topic is to analyse crime related activities concerning illegal export of metal-bearing, in particular electric and electronic equipment waste (WEEE).
Activities should be targeted to:

- understanding the involvement of organized crime in the global distribution of e-waste;
- analyzing criminal activity and crime types associated with illegal e-waste shipments, drawing on other work being carried out targeting illegal e-waste exports on an international scale;
- estimating the true volume of WEEE generated and the amounts inappropriately disposed of;
- assessing the typology of companies (and brokers) involved in the export market and identifying those with a criminal history;
- developing detailed understanding of the destinations and routes used to carry illegal shipments, to possibly enable contacts with regulators and enforcers in destination countries.

This action is expected to identify and propose potential solutions based on a thorough analysis of:

- hurdles and challenges at the source (including the role of local waste sites in the illegal export of electric and electronic equipment waste (WEEE)),
- judicial bottlenecks and strategies for improvement of enforcement.

To analyse and investigate the issues effectively, close co-operation between academic researchers, customs officials, law enforcement agencies is required. The study should have an EU focus, building on the ongoing activities/work of Interpol.

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Coordination and Support Action (coordination action)

**Expected impact:** The challenges relate to the assessment of illegal activities and the present lack of data, and impact should be measured against such background. The action should support intelligence-led policing and advance collective knowledge about crime, organised crime and associated risks. It is expected to benefit and support to different EU policies, including:

- Implementation of the Waste Shipment Regulation
- Implementation of the EU Communication on "Tackling the Challenges in Commodity Markets and Raw Materials"
- Implementation of the WEEE directive, with regard to recycling targets and ambition
- Achievement of recycling targets and objectives in different pieces of legislation
- Generally support to EU 2020 objectives with regard to energy efficiency and resource efficiency.

### *Topic SEC-2012.2.2-2 Air traffic Management/Control threat assessment model - Integration Project*

**Description of topic:**

The EU is funding the development and implementation of a new European Air Traffic Management System through the SESAR (Single European Sky ATM Research) initiative. SESAR provides technology and procedures to enable the air traffic growth by three times, thereby giving due considerations to safety, environmental and societal benefits.

The design of such a new European ATM system must however be complemented with security measures to assure that the correct security level is met; the latter to reflect the requirements stemming out of the global threat scenario. While SESAR already gives due consideration to the definition of security risks that might impact its systems operation (and is developing and validating technologies to provide the security levels needed to protect the future European ATM System) some gaps are still to be covered relevant to the management of aviation threats, incidents and crisis at European level, the protection of the ground ATM infrastructures and personnel, as well as on new emerging threats (such as cyber threats and threats stemming out of the attacks/spoofing to/of the telecommunication systems)

Improvements to ATM security need to be supported in an integrated manner by additional research covering (among others) standards and regulations, procedures, technologies, and training and human factors aspects. Innovative operational scenarios may be proposed covering the whole ATM system, covering the data managed and broadcasted in the satellites, aircraft and ATC centres, the ground infrastructure and the ATM staff, and the management procedures for aviation crisis and incidents. Validation exercises are required to determine the suitability and feasibility of the operational scenarios, assessing the performance and adequateness of the procedures, technologies and staff issues proposed.

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding Schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** The work should lead to a more secure European Air Traffic Management system and complements work already done under SESAR, thereby considering work done in harmonising the civil / military use of airspace (e.g. the activities of the NATO / EUROCONTROL ATM Security Coordinating Group – NEASCOG. Solutions developed under the research work should allow the advantage of speed that is inherent to air transport to be retained; the expected outcome of the activities shall also offer Governments, businesses and industry users a structured turn-key transition plan(s) for implementation of the air space distribution and its management solutions as carried out by SESAR, which shall enable a reliable and secure ATM system capable of efficient security processes and effective handling of incidents at European level avoiding business disruption, shortages and the negative economical consequences.

### *Topic SEC-2012.2.2-3 Improving security in air cargo transport - Integration Project*

**Description of topic:**
Potential security risk to aviation includes those stemming out of shipping dangerous goods as cargo; thus making use of the well developed global cargo distribution network. Explosive devices (such as the laser printer cargo consignment shipped by air from Yemen to US recently) and/or other CBRN material might be entered into the system of air-cargo chain to

get aboard of the aircraft. Once in the airplane they constitute a danger not only to the airplane and its passenger but also to the community as a whole. Mixed cargo and passenger flights are common practice potentially increasing the number of fatalities in case of an exploding cargo.

The purpose of the project is:

- first, to evaluate existing and pending detection technologies and scenarios, as well as strategies for implementing them, for explosive detection (trace and bulk) before boarding cargo and mail onboard aircraft, and
- second, to develop innovative strategic solutions for a European secure air-cargo supply chain noting the EU airports role as international cargo transfer hub, focussed on the implementation of adequate security processes, operational tools and concepts, including the identification of necessary technological means.

Given the complex yet vulnerable environment relevant to aviation security and the implication imposed by air cargo, it is considered essential to follow a systemic approach, building on integration of means and resources, thereby pursuing technological developments that should enable the necessary capabilities to become available for timely and effective prevention, monitoring and reaction on threats stemming out of air cargo.

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** The work should be for the benefit of industry and public authorities to improve the current levels of security, the compliance monitoring, and to facilitate transactions so as to retain the advantage of speed inherent to air transport, thereby optimising costs. The work should be benchmarked on its contribution to the security of citizens in general and that of air travellers, whilst avoiding duplication of measures and disruption in the air-cargo supply chain and related businesses, thus impeding our industry competitiveness.

### *Topic SEC-2012.2.2-4 A common EU aviation security requirement to reduce costs and facilitate passenger flows - Coordination and Support Action*

**Description of topic:**
In order to maintain a high and even performance level of aviation security, EU legislation sets common basic requirements. Over time, however, the latter have frequently been amended, resulting to the costs to safeguarding this high performance level to steadily increase and by now it forms a very substantial part of aviation industry expenses. In addition, passengers may face longer and more complicated procedures at security checkpoints. Amendments have been posed upon previous amendments, thus creating layers upon layers of requirements that are not necessarily harmonious in a single design. Driven by incidents, ever increasing security levels have a huge impact on passengers, the aviation business itself and those businesses that depend on air transport. Today, between 25 and 33% of airport operational costs are related to security measures. Passengers and cargo shippers are dissatisfied with the existing security procedures due to poor service, loss of time, high costs, and possible health concerns and an increasing loss of privacy.

A new aviation security requirement should combine a positive passenger experience and high service level while delivering adaptable, more reliable, flexible and cost-effective security. The review should also identify the relationship between the quality and proficiency of screening processes and the role of private and public entities involved in screening performance.

In order to maintain high levels of security in the future, whilst preventing another increase in the costs for the industry and to be facilitating to the passengers, innovative research should focus on how to achieve this. In particular, a review of detection technologies noting the evolving threats should be undertaken in passenger, cabin and hold baggage screening and processing areas. Processes such as unpredictability in the field of passenger screening should be further evaluated and developed in view of use of such methods in other states, notably US.

Projects may also serve a broader purpose, for instance on how different airport processes (security, safety, border controls etc) can be integrated to achieve the topic aims. Cost/benefit considerations should be discussed.

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Coordination and Support Action (coordination action)

**Expected impact:** The results of the project will contribute to further improve EU common basic requirements for aviation security whilst reducing security costs and time needed for security measures. It should support the EU aviation industry, the security staff and be of benefit to the air travellers. A strong participation from the end user's side is also recommended.

***Area: 10.2.3 Surveillance***

### *Topic SEC-2012.2.3-1 Early warning security systems: physical protection of critical buildings - Capability Project*

**Description of topic:**
Current day physical security systems, including those for the protection of critical infrastructure are reactive i.e., they react to perimeter breaches or intrusions after they have occurred. Extending the “security zone” beyond the critical perimeter, both for terrestrial and air borne, would allow early warning and monitoring of intention, but it could also make the system more prone to false alarms. Advanced security systems that can anticipate physical intrusion or breaches before they occur can greatly reduce the likelihood and extent of damage. Identification of suspicious activity using risk based approaches and development of advanced intrusion device are some of the elements in this solution space. The system should be also privacy respectful, trying to reduce both the image based systems and physical obstacles (as fences) needs. These intrusion devices should also have the intelligence to distinguish between animals, humans, vehicles (land or air borne).

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Improved critical infrastructure protection and effective management of false alarms, including testing, validation and demonstration of the proposed solutions.

***Area: 10.2.4 Supply chain***

### *Topic SEC-2012.2.4-1 Pre-normative technology development for improved and more efficient security of the supply chain - Coordination and Support Action*

**Description of topic:**
In recent years, significant legal and structural developments have taken place to improve the security and safety of international supply chains and movement of goods crossing the EU border. The Common Risk Management Framework (CRMF), implemented by customs authorities, entails continuous screening of electronic pre-arrival (and pre-departure) trade data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately. The CRMF also provides for application of more intensive controls targeting identified priority areas, including trade policy and financial risks.

The EU and its Member States are committed to implementing the global standard set by the WCO (World Customs Organisation) SAFE Framework and its end-to-end supply chain security concept, in particular following its security amendments to EU customs legislation (Regulation 648/2005 and IP 1875/2006). Modern technology is one of the cornerstones to enable Customs to adopt modern risk management working methods resulting in more efficient freight screening and reduction of physical inspections.

The aim of this coordination and support action is to prepare the way towards roadmapping specific future EU technology pre-normative R&D projects. It should take into account the work being undertaken by the expert group on detection technology set up by the EU under Customs 2013 programme to explore and define the needs for new and improved tools or equipment.

The action should liaise with the WCO Scientific Committee and other relevant committees, involve other international bodies and the private sector (i.e. shipping companies) that operates in the Supply Chain, with a view to promote the take up of technology which is suitable on globl scale and practicable for a whole range stakeholders, into common standards, procedures and interoperability. Proposals should take into account as much as possible relevant, existing, past or ongoing research projects.

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Coordination and Support Action (coordination action)

**Expected impact:** Securing the global supply chain is a major element in securing both the lives of people and the stability of the economy. The WCO adopted a series of measures for a framework of international best practices and standards to be used by its Members in securing the international trade supply chain while facilitating the flow of legitimate trade and implementing their national requirements. The EU is the major trading partner of the world.

European stakeholders, in collaboration with other global trading partners, are expected to influence the work on standardization in the field of Supply Chain Security in particular at ISO level. The impact of this action shall be measured against this background.

***Area: 10.2.5 Cyber crime***

### *Topic SEC-2012.2.5-1 Convergence of physical and cyber security - Capability Project*

**Description of topic:**
Increasing demand for tight control and access within closed environments is accompanied with a need for clear evidence as to where and how systems have been accessed. The key is that security operators can not only prove who has accessed a system, but also supply proof that employees have found themselves at a specific location when system access occurred. Example areas range from major sport events to critical infrastructure protection, amongst others. This topic is related to many physical and logical security services that have to be deployed in both physical and electronic domains to achieve a consistent and irrefutable record of who did what, where and when. Both domains, for example, contain services such as access control or information correlation that could and should be integrated. The emphasis should be on increased efficiency whilst addressing societal and privacy needs.

An increasing amount of physical-security systems are cyber-enabled, offering a way to merge with existing cyber-networks, or at least establish a separate IP network. There are already good examples, such as common identity-management system. In certain situations it is not only useful, but also necessary to gather information from one domain, e.g. from physical-security, and to use it as risk and threat factors in logical IT security risk assessment. Need for convergence is also evident in any other directions: cyber threats are global and their management is affecting local physical security. The multi-sectoral aspects of a cyber attack should be taken into account.

Proposers for this topic should look for an enhanced SME participation as described in Part I of the Work Programme.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** One of the problems that citizen perceive today is the fragmentation of security approaches, event and information management, etc. Addressing cross-sector issues and optimization of converged risk management will not only enhance overall security of citizens but, in terms of efficiency and coherence, will improve perception of citizens.

### *Topic SEC-2012.2.5-2 Cyber resilience – Secure cloud computing for critical infrastructure - Capability Project*

**Description of topic:**
Cloud computing will change computing environments as we know them today. With the increasing use of this model which provides computing functions as a utility, more and more

sectors will incorporate cloud services in the computing environment, eventually reaching ICT services which are operating critical infrastructures (e.g. telecommunication networks). The advantages of this new technology can not be neglected, and commercial pressure will contribute to a widespread adoption. The objective of this topic is to analyse and evaluate cloud computing technologies with respect to potential security weaknesses in sensitive environments, and to further develop new technologies for implementing high assurance clouds. Trustable cloud computing systems and scenarios have to be developed, to allow sensitive applications to leverage the potentials of this new technology. Work done on this topic has to take into account existing research on cloud computing technologies, and take it beyond state-of-the-art level towards trustworthy cloud computing. Furthermore, it is necessary to assure the societal acceptance of solutions produced by the project. Important topics of research include, but are not limited to:

- Data confidentiality in the cloud: one has to analyse how distributed systems can be built with cloud services that provide end-to-end data confidentiality.
- Security in large scale cross-organizational systems: how can existing security mechanisms like security policy enforcement, identity and access management, incident response handling or auditing be adopted in large scale cloud environments.
- Best practices for security in cloud computing for critical infrastructure ICT.

**Funding scheme** Collaborative Project (small or medium-scale focused research project),

**Expected impact**: With the adoption of cloud computing in critical infrastructure, the results of this work should make sure that these new technologies do not introduce new weaknesses into these systems, but should increase knowledge of the impacts and consequences of these technologies which will allow critical infrastructure operators and manufacturers to leverage their advantages without sacrificing system security. Furthermore testing, validation and demonstration of these technologies should be foreseen.

## *Activity: 10.3 Intelligent surveillance and enhancing border security*

Actions in this activity will deal with issues relevant to all the consecutive tiers of European border security strategy, starting with visa application procedures in embassies and consular posts (1st level), cross-border cooperation (2nd level), measures at the border crossing points at land borders, harbours and airports as well as between the border crossing points at green and blue borders (3rd level) and finally activities inside the European external borders (4th level) such as exchange of information, compensatory measures, Schengen Information System (SIS), Judicial and Police, Customs and Border Guard cooperation (PCB). A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases ‘identify’, ‘prevent’ and ‘protect’. The ambition is both to avoid an incident and to mitigate its potential consequences.

To build up the required capabilities, emphasis will be on issues such as: enhancing the effectiveness and efficiency of all security relevant systems, equipment, tools and processes used at border crossing points (e.g. identification of accessing people, non-invasive detection of people and goods, tracking of substances, sampling, spatial recognition including data capture and analysis, etc.); improving the security of Europe’s land and sea borders (e.g. through non invasive and underwater detection of vehicles, tracking of vehicles, spatial recognition including data capture and analysis, surveillance, remote operations, etc.); maritime security; assessment and management of (illegal) migration flows. A suitable

framework will be established to coordinate with the activities of the European Agency for the Management of Operational Cooperation at the External Borders[25].

This activity is divided among five areas: **Sea borders; Land borders; Air borders; Border checks; Border intelligent surveillance.**

***Area: 10.3.1 Sea borders***

### *Topic SEC-2012.3.1-1 Increasing trustworthiness of vessel reporting systems - Capability Project*

**Description of topic:**
This topic relates to maritime security, control and law enforcement, including identification of possible polluting ships or illegal fishing vessels. Ship reporting systems (mainly LRIT, VMS and AIS) are today the backbone of maritime surveillance, control, safety and security. However their contents can be faked (spoofed) by malevolent operators. Research is needed into techniques to verify the sources of these messages, for instance by reception and analysis of the emitted radio signals or fusing with intrinsic vessel properties data (magnetic and/or acoustic signatures; dimensions). This should also take into account the use of ship navigation radar for ship detection and tracking. Space-based sensors could be used as a complement (not exclusively).

Recent and ongoing developments in the EU are aimed at strengthening maritime surveillance, because of perceived threats to the security of the maritime domain. Maritime domain awareness is achieved by combining vessel traffic information from many sources, both cooperative (reporting) and non-cooperative (observation).

However, the data of the reporting systems is taken currently for the most part at face value. As soon as the maritime domain awareness is operational on the above principles, malvolent operators could take counter-measures. One likely and powerful counter-measure is spoofing the vessel reporting systems. Spoofing (i.e., wilfully transmitting false information) is already occurring now in particular and still rare situations. Therefore, the authorities in the EU, at MS and EU-level, need to be ahead of this potential security hole by evolving counter-spoofing methods. As it concerns EU-wide and even global systems, counter-measures should be developed at EU (and global) scale.

The project would anticipate the need to further verify (double-check) ship reporting systems. It should analyze possible different approaches and identify the most appropriate ones (e.g. including the transmission of verification signals on the same or another channel, handshaking protocols, use of encrypted signals, physical protection of the transmitters, independent localisation of the transmitters by Radio Frequency techniques, making use of data that are only locally available such as GNSS signal phase shifts, etc). If appropriate, different solutions could be examined in separate work packages.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

[25] FRONTEX

**Expected impact:** The results of this project are expected to close a gap in the security of the maritime domain, with indirect benefits in curbing smuggling of narcotics and other material, illegal immigration, terrorism, illegal fishing, etc.

### *Topic SEC-2012.3.1-2 Pre-Operational Validation (POV) at EU level of common application of surveillance tools*

**Description of topic:**
The Security Research Theme aims to promote further cooperation between public authorities for getting new solutions developed to improve the quality and efficiency of public services related to security, on topics of common European interest, through the pre-operational validation (POV) of such services. Pre-operational validation guided by potential end-users allows a tangible assessment of the performance levels offered by innovative technologies in a realistic user-defined operational scenario, where a trade off between efficiency, effectiveness and cost can be aligned with actual needs. Moreover, pre-operational validation allows, not only the assessment of a stand-alone technology, but also the assessment of the integration of the new capabilities provided into current surveillance infrastructure at all levels in the systems' lifecycle (from technical to logistics, training, maintenance, operation and disengagement).

The close link between end-users and industry, especially in those cases where there is a fuzzy perception of the real needs of the user in daily practise for a particular technology, will extend the benefits of pre-operational validation beyond technical development. The identification of innovative applications, business models and procurement strategies will reverberate in the integration of innovative solutions as fully operational tool. By acting as technologically knowledgeable validator of new R&D, the public demand side can drive innovation.

Last but not least, the activities carried out under pre-operational validation shall put in common, in an experimental framework, the achievements of previous initiatives that have explored and studied the different dimensions of components and systems, from the pure technological development to the features of its exploitation.

In particular, as part of Activity 10.3 (*Intelligent Surveillance and enhancing Border Security*), this topic is presented for proposals to enhance the use by the concerned civilian authorities of innovative technology for border surveillance.[26] The specific objective of this topic is to address solutions for the pre-operational validation of "*Common Application of Surveillance Tools at EU level*".[27]

The overall objective is to provide the EU with an operational and technical framework that would increase situational awareness and improve the reaction capability of authorities surveying the external borders of the EU. A decentralised approach should be followed with

[26] The Commission recently indicated such objective in its communication "EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final)).
[27] Further guidelines and relevant policy background in the area of Security, including concerning the European Border Surveillance System (EUROSUR) and its 2011 concept of operations for the common application of surveillance tools, can be obtained from the dedicated Security Research web-site of EUROPA http://ec.europa.eu/enterprise/security/index_en.htm.

national key players in its implementation. Only selected elements of a European approach to Border Surveillance are to be done at European level, in line with the principle of subsidiarity.

New security solutions to be validated under this action should take into account any aspect of border security that could threaten human rights or break international law. When necessary and appropriate, alternative solutions should also be explored.

The topic proposed is to be implemented via the CP-CSA funding instrument, which involves a combination of the collaborative project and coordination and support action funding schemes. It enables therefore the financing, under the same grant agreement, of research, coordination and support activities.

Its aim is to both enable public authorities in charge of border surveillance to innovate faster in the provision of their institutional services, making them more efficient and effective, and also increase the research capacity and innovation performance of European companies and research institutions, creating new opportunities to take international leadership in new markets.

This CP-CSA for POV will combine two components with synergistic effects:

a. Networking and coordination activities: for public bodies in Europe to cooperate in the innovation of their public services through a strategy that includes POV.
b. Joint research activities: related to validating the POV strategy jointly defined by the public bodies participating in the action. This would include the exploration of possible solutions for the targeted improvements in border surveillance services, and the testing of these solutions against a set of jointly defined concepts of operations and performance criteria.

This activity requires the participation of at least three independent public authorities in charge of border surveillance (at local, regional, national or supra-national levels), each established in a different Member or Associated State. Other stakeholders may participate in addition, if their participation is well justified and adds value to the action (especially if they represent an authority or a regulatory body with responsibility in some area affected by the use of a particular technology).

**SCOPE of the CP-CSA (**Collaborative Project and Coordination and Support Action**)**

In the context of European Border Surveillance, this CP-CSA is to conduct pre-operational validation of common applications of surveillance tools at EU level via the competitive testing and assessment of several potential solutions. Tools to be tested may include a variety of platform types deploying sensors for surveillance purposes.[28]

The information acquired by each platform type should be correlated with ship reporting systems and other available intelligence sources (i.e. satellite imagery, sensor data or open source information) to provide the relevant national and European Agencies with surveillance information on their external borders and the EU pre-frontier area on a frequent, reliable and cost-efficient basis.

The specific objective of the competitive testing will be to assess:

[28] It should be noted that development of space-based observation and assessment tools for border surveillance is undertaken in the WP for Theme 9 ‘Space’ (Area 9.1.1.).

- the identification of the different technological alternatives for the achievement of a set of user-defined operational objectives;
- the technical feasibility of alternative options for the Common Applications of different types of surveillance tools;
- the feasibility of the integration of these technologies taking into consideration the limitations imposed by the existing surveillance deployments and the current use of segregated and non segregated airspace;
- the comparative performance of proposed options, while deployed in daily operations in real scenarios;
- the identification and documentation, as appropriate, of the infrastructure, capabilities and skills required for the acquisition and operation of these systems under user-defined safety and security conditions;
- the cost-benefit ratio of each of the options tested within each of the two types of tools;
- the identification of the maturity level showed by both solutions in order to promote short/mid term utilisation;
- the definition of innovative applications, business models and procurement schemes that can facilitate the migration to these new solutions from the existing traditional tools.

The overall validation action **CP-CSA** is to be divided in the following three phases.

**1) Initial Definition Phase (CSA):**

The definition phase should be based on the latest relevant requirements for European Border Surveillance. Participating border surveillance Authorities are expected to present their cooperative plan for definition of the later phases, in coordination with other relevant EU organizations.

In this phase a strategy shall be put in place for:
- Identification of elements requiring new R&D that could be tested and validated in cooperation,
- Definition of an action plan, setting scenarios and issues for concrete implementation of activities,
- Establishment of good practice procedures for POV evaluation and monitoring (common evaluation criteria and implementation methods),
- Drafting a preliminary IPR strategy for the (expected) outcome of the Call for Tender in phase 2, taking into account the provisions set out in the Appendix,
- Allocation and training of additional resources for implementation (if appropriate),
- Building cooperation with other stakeholders (if appropriate).

The outcome is expected to be a Validation Strategy Document, including a practical Exercise Plan for the actual testing phase, to be used for the definition of the specifications of a joint POV Call for Tender for the subsequent execution phase, setting the rules for participation, the criteria to evaluate competitive tenders, and for selection/award. Such call shall be defined in such a way that it respects the Treaty principles and the specific requirements in Appendix.

**2) Preparatory Work and Execution Phase (CP):**

This phase will implement the strategy and action plan as prescribed by the participating authorities, in Phase 1 (in particular the Call for Tender for the implementation of testing). In this phase the providers of solutions to be tested (at least two for each scenario), are to be

selected via the competitive call as defined in phase 1. These providers will execute the testing of their systems according to the prescription of the action plan, working under the supervision of the concerned national Border Authorities. The testing Exercise Plan is expected to be contracted along 2013-2014.

**3) Final Ex-post Assessment Phase (CSA):**

In this phase, which will conclude the overall validation, participating national Border Authorities, in coordination with other relevant EU organizations, will conduct a thorough assessment of the solution performances as demonstrated in the testing exercises of phase 2, against the set of jointly defined performance criteria, in order to verify fitness for purpose, with a view to a potential conversion into permanent services of the systems tested. This phase should confirm as appropriate the IPR strategy and include dissemination of results to standardisation bodies (if appropriate). This ex-post assessment of the outcome of each scenario is to be implemented in the first half of 2015.

For implementing this CP-CSA, different constellations for joint validation[29] are allowed, such as for example common validation entity[30], lead authority[31] and piggy-backing[32] constellations.

**EU CONTRIBUTION**

The EU contribution shall take the form of a grant that will combine the reimbursement of:

- 100% of the total eligible costs (the reimbursement of the indirect cost may reach a maximum of 7% of the direct eligible cost) of the participating authorities for the activities linked to the preparation, definition, management and coordination of the joint POV Call for Tender (CSA phase 1),
- maximum 50% of the total eligible costs for the research and technological development activities charged by the providers of solutions to be tested (75% in case of "*Market failure and of accelerated equipment development*"[33]) (CP phase 2) and
- 100% of the total eligible costs (the reimbursement of the indirect cost may reach a maximum of 7% of the direct eligible cost) of the participating authorities for the activities linked to the final validation of the outcome of the execution phase (CSA phase 3).

[29] "Joint validation" means combining the validation actions of two or more contracting authorities. The key defining characteristic is that there should be only one tender published on behalf of all participating authorities.

[30] The "common validation entity" constellation is an arrangement for joint validation where all involved public authorities commonly establish or designate one external legal entity to conduct the joint validation with a joint mandate and joint resources of all public purchasing authorities.

[31] The "lead authority" constellation is an arrangement for joint validation where a group of public authorities collaborate through their existing departments in such a way that one public authority of the group is designated as lead authority to take responsibility for, tendering and arranging contractual documentation for specific validations, all in consultation with other purchasing authorities involved in the joint validation.

[32] In the "piggy-backing" constellation one public authority executes the validation and provides access to the results of the contract for a wider range of authorities, essentially by stating in the Contract Notice that other named public authorities may also wish to may also wish to make use of the resulting contract a later date (normally during the timeframe of the original contract).

[33] Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013) Art 33.1

It is clear from the above that, in addition to the EU financial support to phase (2), participating Border surveillance authorities shall contribute directly to the research and technological development activities involved in the testing of new solutions.

**Expected impact:** This CSA-CP is expected to significantly contribute to the implementation of a European approach to Border Surveillance, thus enabling national and other relevant authorities to more effectively carry out their border surveillance activities, collaborating at tactical, operational and strategic levels, in order to:
– increase internal security of the EU by preventing cross-border crime;
– reduce the number of irregular migrants;
– considerably reduce the unacceptable death toll of migrants at sea.

At the end of the project, the participating public bodies in charge of border surveillance (also potential purchasers) should have obtained clear evidence of the cost-efficiency of alternative surveillance systems, which could later be deployed as common EU level surveillance applications.

The project is also expected to promote increased opportunities for market uptake and economies of scale for the supply side by forming critical mass on the public demand side, and contribute to standardisation of jointly defined public sector requirements specifications.

**Appendix: Specific Requirements for the implementation of Pre-Operational Validation (POV)**

The following requirements are applicable to POV calls for tender launched under actions requiring POV to ensure that the conditions for the Article 16(f) exemption of the public procurement Directives 2004/18 and Article 13(j) of Directive 2009/81/EC are respected, that the risk-benefit sharing in POV takes place according to market conditions and that the Treaty principles[34] are fully respected throughout the POV process:

- The consortium of public bodies should verify that the topic proposed for the joint POV call for tender would **fit the scope of an R&D**[35] **services contract**[36].
- **The practical set-up foreseen for the POV** shall be clearly announced in the POV contract notice. This shall include the intention to select multiple companies to start the pre-operational validation in parallel, as well as the number of phases and the expected duration of each phase.

[34] In particular the fundamental Treaty principles on the free movement of goods, the free movement of workers, the freedom to provide services, the freedom of establishment and the free movement of capital, as well as the principles deriving there from, such as the principles of non-discrimination, transparency and equal treatment.

[35] R&D can cover activities such as solution exploration and design, prototyping, up to the original development of a limited volume of first products or services in the form of a test series. Original development of a first product or service may include limited production or supply in order to incorporate the results of field testing and to demonstrate that the product or service is suitable for production or supply in quantity to acceptable quality standards. R&D does not include commercial development activities such as quantity production, supply to establish commercial viability or to recover R&D costs, integration, customisation, incremental adaptations and improvements to existing products or processes.

[36] Contracts providing more than only services are still considered a public service contract if the value of the services exceeds that of the products covered by the contract.

- **Functional specifications** shall be used in order to formulate the object of the POV tender as a problem to be solved without prescribing a specific solution approach to be followed.
- In view of triggering tenderers to send in innovative offers that include R&D that can bring breakthrough improvements to the quality and efficiency of public services, the selection of offers shall not be based on lowest price only. The POV contracts shall be awarded to the tenders offering **best value for money**, that is to say, to the tender offering the best price-quality ratio, while taking care to avoid any conflict of interests[37].
- In respect of the Treaty principles the public purchasers shall ensure **EU wide publication** for the POV call for tender[38] in at least English and shall evaluate all offers according to the same objective criteria regardless of the geographic location of company head offices, company size or governance structure. The POV process should be organised so as to stimulate companies to locate a relevant portion of the R&D and operational activities related to the POV contract in the European Economic Area or a country having concluded a Stabilisation and Association Agreement with the EU.
- In POV, the public validator does not reserve the R&D results exclusively for its own use. To ensure that such an arrangement is beneficial both for the public purchaser and for the companies involved in POV, **R&D risks and benefits are shared** between them in such a way that both parties have an incentive to pursue wide commercialisation and take up of the new solutions. Therefore, for POV, ownership rights of **IPRs** generated by a company during the POV contract should be assigned to that company. The public authorities directly contributing to the POV phase (2) should be assigned a free licence to use the R&D results for internal use as well as the right to require participating companies to license IPRs to third parties under fair and reasonable market conditions, to be specified in the Call for Tender. A call-back provision should ensure that IPRs from companies that do not succeed to exploit the IPRs themselves within a given period after the POV project return back to the public bodies in charge of border surveillance.
- In order to enable the public validators to **establish the correct (best value for money) market price for the R&D service, in which case the presence of State aid can in principle be excluded** according to the definition contained in Article 107 of the Treaty on the Functioning of the European Union, the distribution of rights and obligations between public validators and companies participating in the POV, including the allocation of IPRs, shall be published upfront in the POV call for tender documents and the POV call for tender shall be carried out in a competitive and transparent way in line with the Treaty principles which leads to a price according to market conditions, and does not involve any indication of manipulation. The consortium of public purchasers should ensure that the POV contracts with participating companies contain a financial compensation according to market conditions[39] compared to exclusive development price for assigning IPR ownership rights to participating companies, in order for the POV call for tender not to involve State aid.
- The POV contract that will be concluded with each selected organisation shall take the form of **one single framework contract covering all the POV phases**, in which the

[37] For more info refer to Staff Working Document on PCP: SEC (1668) 2007.

[38] Through the Official Journal of the European Union (OJEU), using the TED (Tenders Electronic Daily) web portal.

[39] The financial compensation compared to exclusive development cost should reflect the market value of the benefits received and the risks assumed by the participating company. In case of IPR sharing in POV, the market price of the benefits should reflect the commercialisation opportunities opened up by the IPRs to the company, the associated risks assumed by the company comprise for instance the cost carried by the company for maintaining the IPRs and commercialising the products.

distribution of rights and obligations of the parties is published upfront in the tender documents and which does not involve contract renegotiations on rights and obligations taking place after the choice of participating organisations. This framework contract shall contain an agreement on the future procedure for implementing the different phases (through specific contracts), including the format of the intermediate evaluations after the solution design and prototype development stages that progressively select organisations with the best competing solutions.

***Area: 10.3.2 Land borders***

No specific topic for this area has been planned for this call.

***Area: 10.3.3 Air borders***

No specific topic for this area has been planned for this call.

***Area: 10.3.4 Border checks***

### *Topic 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 - Capability Project*

**Description of topic:**
The EU is strongly committed to enhancing the security of the international supply chain in line with international standards, like the World Customs Organization's SAFE Framework of Standards to secure and facilitate global trade. The WCO (World Customs Organisation) SAFE framework of Standards and the strategic document "*Customs in the 21st Century*" makes clear that the use of modern technology is one of the cornerstones which enables Customs to adopt modern risk management working methods. Customs administrations are encouraged to take advantage of emerging technologies to enhance security in the supply chain

Today, Customs is confronted with a double challenge. On the one hand they have to guarantee the security of the citizen through more effective controls. On the other hand they have to facilitate trade through faster and more streamlined control of merchandise. Meeting these two objectives at the same time is very demanding and requires innovative and cost effective approaches in order to create win – win solutions for both.

Presently the biggest challenge for customs is to interpret and evaluate the x-ray images and find the irregularities particularly in the case of container scanning. Unfortunately manufacturers can provide training only for the technical use of equipment and not for how to select cargo for further control on the basis of the images. Having such system, automatic comparison of X-Ray images with a reference database of previously scanned commodities, were confirmed that no irregularities were detected, would be of great help for customs officers involved in X-Ray inspection and image analyzing.

The following are identified as specific obstacles to overcome:

- shortage of images of detections;
- confidentiality issues;
- different type of software and technical solution used by each manufacturer.

The project should be would be based on historic images of real detections, where similarities are identified and captured and used to trigger an automatic alarm.

This type of application could be developed as software adds on for use by (cargo) scanners manufacturers, or as a training course for customs. The action should explore the possibilities to include generating reference images of illegal cargo mock-ups, as well as reference images of legitimate cargos for comparison purposed.

The build up of a reference database of images of vehicles- cars, trucks, vans etc according to their make &model etc, could also be considered. These could be overlaid on real-time images to check for anomalies.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** The system should be fit for purpose of customs inspectors, and should be appropriately tested and validated by them. It should make possible the automatic comparison and correlation of X-Ray images with database of previously found confirmed legal and illegal commodities, providing reliable and information to customs officers involved in X-Ray inspection and image analyzing. Its use is expected to progressively become en element of a European system; therefore the project should be compatible with any manufacturer system and also cover all the appropriate interoperability (and technology neutral standardization) issues.

### *Topic SEC-2012.3.4-2 Research and validation for fingerprint live scanners - Capability Project*

**Description of topic:**
The overall success of applications using fingerprints for identification and verification purposes greatly depends on the quality of the fingerprints initially enrolled. While livescan technology has improved over the past 15 years, innovative technology has recently been proposed to take fingerprint images by looking at additional biometrics associated with the finger.

Superficial skin disorders like scarring, absence of ridges due to hard manual work, mutilation, etc. would normally lead to very bad fingerprint images using traditional optical techniques. New technologies allow “looking” at additional biometrics associated with the finger that could complement existing fingerprint technology to deliver a high-quality image.

The aim of the project would be to validate among these technologies which ones are best fit for purpose of border control and law enforcement applications (real-live implementations would be required).

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** High fingerprint quality is a pre-requisite for applications like EU-Passport, EURODAC, VIS, Entry/Exit, and Registered Traveller Program to deliver good results and very low error rates. The work should determine which technology(ies) fit for purpose in border control and law enforcement applications.

### *Topic SEC-2012.3.4-3 Tools and processes for assessing the impact of policies/actions on border control - Coordination and Support Action*

**Description of topic:**
The aim of the action is to analyze and propose methodologies, tools & processes for:

a) Identifying, modelling and simulating possible short-term and long-term geopolitical scenarios and their impact on illegal immigration and on the border security level, adopting a holistic approach.
b) Simulating and assessing the impact of policies/actions at different decision levels (European, National and Regional) on illegal immigration and on the border security level.
c) Benchmark the expected performance of different policies/actions (under cost benefit analyses or multi-criteria analysis) for identifying which of these are the most promising, i.e. which of these can achieve the desired level of border security with lower costs (monetary and non-monetary) taking into account social and cultural issues and without breaching the existing constraints (legal, technological, etc...).
d) Apply models and simulations to conduct cost versus operational effectiveness trades and assessments for alternative border security concepts and technologies. Identify and assess the applicability of currently available technologies and systems for deterrence/impedance of border crossing threats; including surveillance, detection and tracking of land and maritime border security threats, communications, command and control systems; and response/ interdiction systems. Work with stakeholders to identify cost effective architectures and concepts of operations.

The building of models is expected to require a multinational approach to data, processes, and performance indicators.

This coordination and support action is expected to provide a clear strategy benchmarking in real time its progress with the concerned EU policy services (DG HOME). It is required that the fitness for purpose of the models and the results will be validated, as appropriate, fully taking into account the responsibilities of national border control authorities/ministries and the Frontex agency.

**Funding schemes:** Coordination and Support Action

**Expected impact:** The Stockholm Action Plan (and the related Internal Security Strategy (in action), strictly linked to the broader European Security Strategy) constitutes the cornerstone of efforts to make Europe more secure by strengthening cooperation in law enforcement and border management, and provides the roadmap to implement policies/actions.

In this context, a balanced migration policy should be put in place addressing the irregular migration problems and, as foreseen in EU 2020, clearing the way for legal migration to the EU, an asset for a sustainable economic recovery.

### *Topic SEC-2012.3.4-4 Innovative, cost-efficient, and reliable technology to detect humans hidden in vehicles/closed compartments - Capability Project*

**Description of topic:**
At present, profiling and detection dogs have proven to be the most effective methods to detect humans hidden in vehicles. Such methods are labour-intensive. Therefore vehicles and containers are not systematically checked for hidden persons.

Technology currently used for detecting humans hidden in vehicles at border crossing points or in in-land mobile checkpoints is either too expensive and potentially problematic from a health and safety perspective (X-ray, gamma-ray), unreliable, or difficult to deploy in all border control scenarios (ex. millimetre wave technology, heartbeat detectors, carbon dioxide probes, laser distance measurement, telescopic inspection mirrors/cameras, electromagnetic field detection etc.).

The aim of this research project is to identify and develop a technology that can detect persons hidden in vehicles/closed compartments with the following characteristics:

- fully automated;
- contactless;
- reliable, with acceptable error/false positive rates (best minimum in comparison to dogs/manual searches);
- robust and resistant to different environments and weather conditions;
- suitable for all types of vehicles and containers;
- fast;
- high throughput;
- cost efficient (acquisition and running costs, staffing requirements);
- compliant with European health and safety regulations;
- can be integrated with other technologies to detect dangerous/illicit materials (ideally in a one-for-all gate through which all vehicles/containers are automatically screened).

Such technology is to be deployed in stationary and mobile (portable, easily deployable) environments (at land and sea borders, for in-land checks).

An appropriate strategy, for the validation of the fitness for purpose of the results of the project, should be foreseen in the proposal taking fully into account the responsibilities of the national border control authorities and the Frontex agency.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Today it is difficult to determine how many illegal migrants use successfully this modus operandi to cross the Schengen borders and arrive to their final destination. The identification of the entry-point into the EU of an illegal immigrant is an essential requirement for the juridical treatment of the case.

This validation strategy should be put in place at the start of the project. Validating authorities should be given the power to stop the project (at any stage) were they to consider developments not sufficiently promising. In addition, as current practices in the Member States/Associated Countries include the use of a combination of the above-mentioned technologies, border guards and customs authorities often share equipments and cooperate

very closely. The impact of the project should be also measured in terms of its interoperability potential.

### *Topic SEC-2012.3.4-5 Further research and pilot implementation of Terahertz detection techniques (T-Ray) - Capability Project*

**Description of topic:**

Non-intrusive, safe and accurate harmful substance / object detection is a prime requirement for border control applications and security. The border passage time is greatly influenced by the baggage and security checks and airports in particular are constantly looking for ways to reduce the time needed for these checks while maintaining or increasing the level of detection features.

Electromagnetic waves up to 1 THz penetrate clothing and can be used for detection of concealed objects. Systems at millimetre-wave frequencies below 300GHz in the lower part of the frequency range have been developed and are in use. Higher frequency systems, in the submillimetre-wave or terahertz region can give better image resolution. Since the emission, absorption, reflection and scattering of materials are all frequency dependent, the use of multiple frequencies is also expected to improve the discrimination of objects in an image – much like the advantage of colour photography over black and white.

Improved image information will enable the development of more effective automatic threat recognition algorithms which, by removing the need for image interpretation by human operators, effectively mitigates potential privacy issues.

The project should develop a prototype imaging system operating at a single or multiple frequencies, including frequencies above 300 GHz. The system must be safe for use on the general public and allow concepts of operation which respect privacy.

The research project is aimed at delivering applications that produce consistent and secure results in operational settings, e.g. in a high throughput aviation security or border control context, or for constant discreet surveillance in high-risk public areas. It would create an image of different substances and objects, with potentially harmful concealed objects (e.g. weapons, explosives) revealed due to their different materials properties. In addition to the development of a system, a demonstrator/pilot test/validation should be implemented in a live operational environment, such as a pilot airport.

**Funding scheme**: Collaborative Project (small or medium-scale focused research project)

**Expected Impact:** Airport, aircraft and border control security are important topics commonly shared by the majority of citizens. Unfortunately, they regularly come into conflict with the simplified and facilitated airport experience desired, as well as required, by all travellers.

The EU VIS (Visa Information System), Automated Border Control gates, and EU Registered Traveller programme all intend to streamline, shorten and improve border control. These programs will all fall short if security checks become longer and longer.

### *Topic SEC-2012.3.4-6 Enhancing the workflow and functionalities of Automated Border Control (ABC) gates - Integration Project*

**Description of topic:**
The EU Smart Borders initiative includes establishing a Registered Traveller Programme in order to facilitate border crossings for third country nationals at EU external border crossing points. The current Automated Border Control (ABC) gates at some EU external border crossing points regularly use only one biometric identifier (face or fingerprints) and can only be used by EU citizens holding e-Passports or National ID Cards. The future development of EU policy will require processing frequent third country travellers at the external border crossing points by verifying their biometrics during the ABC process. It is also expected that EU citizens will be able to make use of ABC gates by using their second generation e-passports containing biometrics, the use of which improves border control procedures by automating both the required identity verification of the passport holder and the required checks. In this way border control efficiency will be enhanced and border crossings facilitated by streamlining processes and allowing Schengen countries to focus their border control resources on other, more security-related tasks and/or to serve other travellers.

The second generation e-passport being issued by Member States includes two types of biometrics: a digital facial image and two fingerprints. Within this context, both types of biometrics contained in the 2nd generation e-Passport are expected to be tested.

However, automated border control systems are being implemented by some Member States at certain external border crossing points to allow for automated border control checks based only on facial recognition using the e-passport. These systems currently do not implement fingerprint verification functionalities (except in very few national registered traveller pilots/programmes). In addition, the design of the user interface is not being harmonised among Member States.

This pilot project should address these two issues. Its objective would be to propose a harmonised and coherent solution, allowing using the second-generation e-Passport to its fullest potential in ABC gates, in particular by testing fingerprint verification functionality in ABC gates.

Attention should be given to compliance with European societal values and citizens' rights, including privacy and acceptability.

Institutions of several Member States are expected to be involved in the case of large-scale pilot project involving different border crossing points and all types of borders. The project is expected to be substantial in size in order to achieve meaningful progress.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** Adopting a common approach to ABCs using biometrics across the EU would allow both EU citizens and third country nationals to experience a more secure and seamless border crossing and will allow border control authorities to better manage and control passenger flows at the external border crossing points. Currently, such a common

approach by Member States to the design of the user interface of ABC gates in particular, which the traveller sees when approaching an ABC gate, is missing.

The project is expected to contribute towards a common European more harmonised approach, improving the workflow and functionalities of ABC gates, at those border crossing points that have this infrastructure in place (and will more and more so in the future). Both border control authorities and travellers (preferably with their second generation e-passports) reaping the benefits of time and resource savings. This project addresses the priorities in the Stockholm Programme and is in line with the strategic objectives of the EU. Its impact should be measured in terms of potential for harmonisation and interoperability at the European level.

***Area: 10.3.5 Border intelligent surveillance***

## *Topic SEC-2012.3.5-1 Development of airborne sensors and data link - Integration Project*

**Description of topic:**
EU Member States, in particular those bordering the Mediterranean, suffer frequent incursions, attempted border crossings and illegal entry. This research should enhance the EU's border security and defences against such attempts.

The EU Internal Security Strategy (in Action) [40] foresees the strengthening of security through border management as one of its 5 objectives. With the Lisbon treaty the EU is tasked to play an active role in treating migration management and the fight against crime

Aircraft and Unmanned Aerial Vehicles (UAVs) are a valuable asset to contribute to law enforcement and immigration control.

Research is needed to enhance their capabilities for their gradual take-up and for improved operational use, in order to conduct maritime and terrestrial surveillance to protect EU borders, for situation awareness (in particular for identification of targets, and of intended incursions into EU territory or territorial waters).

This project is therefore aimed at the development of optimum airborne (i.e. optics/ optronics and 3D) sensors and associated data analysis, when the mission is to conduct effective surveillance over a large maritime or terrestrial area in a fixed time combining large field and focused/tracking surveillance capabilities and the development of an adapted data link using civilian frequencies and protocols.

One of the main issues for airborne sensors effectiveness and operational capacities is to offer large and focus capacities.

[40] See:
http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

In this sensor development, the specific constraints for applicability in a civil security related scenario should be taken into account (miniaturization, affordability, endurance, resolution, mission timing and characteristics, operating procedures).

The project should also cover all the appropriate interoperability (and standardization) issues.

Attention should be given to compliance with European societal values and citizens' rights, including privacy and acceptability.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** The project is expected to contribute to the implementation of step 4 of the European Border Surveillance system (EUROSUR), via the improvement/use of surveillance tools for border surveillance. The solution(s) developed will have to be tested (possibly airborne) and validated with regard to technical feasibility and cost-benefit ratio.

## *Activity: 10.4 Restoring security and safety in case of crisis*

Actions in this activity will focus on technologies providing an overview of, and support for diverse emergency management operations, such as in civil protection (including natural disasters and industrial accidents), humanitarian aid and rescue tasks. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases 'prepare', 'respond' and 'recover'. The ambition is to mitigate the consequences of the incident. To build up the required capabilities, emphasis will be on issues such as: general organisational and operational preparedness to cope with security incidents (e.g. inter-organisational coordination and emergency communication, assessment of strategic reserves, strategic inventories, etc.), crisis management (e.g. integrated means of alert and management, assessment of the incident and priority requirements, integration of heterogeneous actors and resources, evacuation and isolation, neutralisation and containment of effects of terrorist attacks and crime, etc.), intervention in hostile environment, emergency humanitarian aid and the management of the consequences and cascading effects of a security incident (e.g. the functioning of the public health care system, business continuity, confidence building measures, restoring the disrupted or destroyed functioning of society, etc.).

This activity is divided among four areas: **Preparedness, prevention, mitigation and planning; Response; Recovery; CBRN Response.**

***Area: 10.4.1 Preparedness, prevention, mitigation and planning***

### *Topic SEC-2012.4.1-1 Preparedness for and management of large scale fires - Integration Project*

**Description of topic:**
Large scale fire events have become in recent years a recurrent phenomena resulting in deaths, major economic loss and long lasting effects on communities. Fire fighting techniques have evolved over the years, introducing fire propagation models, fire retardant materials, air

fighting among others. These tools needs to be adapted to the reality of people living in what used to be only forest, what makes the "safety barriers" smaller and at the same time the fires more violent and more frequent. There is also need to integrate into the fire fighting arena tools such as air and land space observations, as well as information to the public affected by the phenomena. Health aspects of the incident and the fire fighting as well as the environmental aspects (including the dispersal of toxic materials, held in facilities affected by the fire)have to be studied. The legal and ethical aspects of the measures used in the management of the incident (e.g. mandatory evacuation, and the use of force to enforce this evacuation) have to be highlighted. Since this type of incidents often requires international cooperation, interoperability issues both in equipment as well as in common operations procedures (between countries) should be studied, and standardisation activities suggested.

Three major scenarios for such events might be considered:
(1) Fires that damage critical infrastructure or industrial facilities
(2) Forest fires (including fires spread outside of the EU)
(3) Fires that can spread in dense urban areas (“city fires”)

Areas to be addressed in research (for all three types of events):

(i) Real time risk analysis
(ii) Fire monitoring
(iii) Disaster management, operational and tactical response
(iv) Innovative passive and active protection measures, with emphasis on active fire protection
(v) Predictive models for fire propagation and fire control

Critical infrastructures to be considered:

(i) Transport (airports, railway terminals, metro and tunnels)
(ii) Communication (TV and mobile transmitters, internet hubs, large computer rooms)
(iii) Energy (power plants, including nuclear, oil refineries, chemical plants)

Objective:

- To develop better tools for fighting mega-fire (especially mega bush fires threatening the public and their livelihoods). These tools should include – modelling tools, monitoring tools and technologies, fire fighting technologies and tools, standard operating procedures, information to the public, public behavioural models, health risks (from the fire retardant materials, to the responders, general public), ethical and legal aspects, environmental impact.
- To develop advanced monitoring tools over large forest areas in order to fast detect and accurately locate fire;
- To develop modelling tools to estimate the progress of a fire (wind and meteorological conditions are of paramount importance in the model) and to indicate highest probability of fire focal points
- To develop situational awareness tools for the command room and the field forces
- To develop methods and procedures to effectively plan and supervise international forces collaboration (including coordination of aerial fleet over relatively small areas). Seamless coordination of the aerial operation and the ground operation is mandatory.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** Better methods for fighting mega fires will make the European citizens safer. Having a comprehensive tool for the management of mega fires (including, health, environmental, legal and ethical aspects), should increase the efficiency of the management of this type of incidents. Besides the project should improve preventative measures, enhance the use of predictive modelling ensuring greater resilience, enabling better response, and addressing issues of standardisation and interoperability across Europe.

### *Topic SEC-2012.4.1-2 Psycho social support in Crisis Management - Capability Project*

**Description of topic:**
Affected public and crisis responders have to deal with different forms of stress and other psycho-social strains and trauma; in order to reduce the short-, mid- and long-term consequences of the various forms of stress and psycho-social strains, psycho-social support should be provided in a timely and professional way. Responders will be confronted with injured, mutilated, traumatised persons and probably also fatalities. External circumstances such as the extent of the devastation, suddenness, force and brutality of the incident, or suspected contamination, may intensify impressions. However, the community in a larger sense and society itself may be affected and suffer from the event which might bear larger cultural, societal consequences and losses, for which support should also be provided.

Thus psycho-social support is not only relevant during the crisis itself, but also afterwards during the recovery phase, sometimes even for the long-term, and may have to extend well beyond the persons directly impacted, such as first responders and the victims and public on the scene, and those indirectly impacted such as family members and para-medical and medical personnel, to a larger audience who might be witness to the incident through media and internet reports. The immediate impact and effect over time of stress and traumatic stress on response forces and crisis management personnel and authorities should also be taken into account. All these elements may have an effect on the dimension, magnitude, duration and repercussions (including delayed repercussions) of a crisis.

Research should identify coping mechanisms and methods to be used by decision makers and responders to minimise effects of stress on themselves and the affected public. The proposers should also develop scenarios for the deployment of effective scenarios of medical and psycho-social intervention forces. Following an analysis of existing approaches and best practices, effective intervention strategies and related support should be developed.

Bottom-up strategies - built up on the capabilities and know-how present on the ground - and effective intervention techniques using adequately trained laypersons instead of professional personnel - who might be scarce - should also be developed.

Objective:

- To develop effective methods and tools for medical and psycho-social intervention for victims, intervention forces and volunteers as well as for the larger community during and after a crisis situation, including
    - Immediate/post-immediate psychological support (acute stress reactions),
    - Treatment of long-term consequences (trauma and PTSD - Post-Traumatic Stress Disorder);

- To improve psycho-medical preparedness for crisis situations (contingency planning for the early interventions, readiness of medical supplies and hospital facilities, determining training and intervention strategies to deal with stress during preparation, response and recovery phases,
- To develop tools able to assess the relationship between the level of stress of the Crisis Managers and the effectiveness of the whole Crisis Management System;
- To develop technologies and effective methods to provide social support to large numbers of people;
- To develop assessment tools for psychological fitness of crisis management personnel and authorities;
- To 'help the people help themselves', that is: to validate and support efforts at local level;
- To identify longer term psychological, societal and cultural impact of crises.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Improved psycho-social preparedness of the public and of decision makers, first responders for crisis situations, effective interventions and appropriate treatment of people affected by psycho-traumatic problems resulting from disasters, societal recovery from, and cultural integration of, traumatic events.

***Area: 10.4.2 Response***

### *Topic SEC-2012.4.2-1 Positioning and timing tools to guarantee security assets trace & tracking together with worker safety in a secure environment - Capability Project*

**Description of topic:**
Disaster prevention and mitigation is a subject to which currently intensive attention is devoted to obtain the main goal to identify efficient ways to inform people at risk and to take specific actions to mitigate disaster's effect with the aim to save lives.

In the context of crisis management, satellite technology can be one of the key elements in relation to the fact that often the disasters have a large-scale and affect the poor and socially disadvantaged in developing countries. This technology complemented by ground based Information systems (Network RTK (Real Time Kinematic); GNSS and EGNOS) may constitute a world wide monitoring and alerting system.

The task is to develop a precise tracking and timing system to be used in case of major failure of existing networks (communications and power) which could be used to localise a) critical assets (such as; trucks, trains, vessels etc.) but also b) first responders, taking into account the internal security of the developed system. An analysis of the security threats to all the elements (hardware, software, communication channel, operating modes, etc.) used in the system should be provided. The developed technology should be compliant with the two main uses described above a) and b).

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** To develop capabilities for tracking/tracing and positioning systems based on the use of existing technologies and applications (Galileo, GNSS) support and ensure safety of crisis management operations.

### *Topic SEC-2012.4.2-2 Situational awareness guidance and evacuation systems for large crowds, including crowds unpredictable behaviour - Integration Project*

**Description of topic:**

Guiding people out of dangerous areas safely is one of the first priorities in cases of a dangerous incident. As such situations are commonly characterized by uncertainty regarding both the source of danger and human behaviour.

Persons involved in a crisis suffer from limited situational awareness (SA). SA involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives. Lacking SA or having inadequate SA has been identified as one of the primary factors in accidents attributed to human error.

The situation awareness system should harness various sensors to perceive the situation, to calculate the development of the situation, and to guide people away safely from the source of danger. Thereby, human behaviour during an evacuation has to be considered.

Incidents typically involve also reactions of society which are difficult to predict let alone control. Mass hysteria may heavily complicate any incident, especially when unconventional and invisible materials such as chemicals, radioactive substances and pathogens are involved.

**Objective:**

- To develop a situation aware evacuation system that is able to adapt dynamically to changing situations.
- To develop integration of multiple information sources leading to enhanced situation awareness to be available to command posts as they are usually not disseminated to deployed intervention personnel.
- To develop a system that will enable sharing all relevant multi-media data – video (including 3D), pictures, voice, force locations, plans, orders, messaging etc. between all operating personnel, including the integration of information, with their command posts and headquarters. The user interfaces, devices and communication should be appropriate for deployed personnel in urban environments.
- To develop a system applicable to a broad range of areas (e.g. large gatherings on fenced/confined outdoor areas, office buildings, underground stations, airports) and to various incidents (natural and man-made as well as terrorism). Therefore the equipment and devices have to be mobile. Furthermore, the system should be capable of providing situational data to first responders and to the general public involved in various forms.
- To develop respective optimal evacuation strategy.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** A system and evacuation strategy which guides people from the dangerous situations. A system that enhances the effectiveness of forces responding to crisis can, reducing time, human error, and collateral damage in restoring security as a crisis unfolds.

### *Topic SEC-2012.4.2-3 Post crisis lesson learned exercise - Coordination and Support Action*

**Description of topic:**
Europe has responded to a number of (natural) disasters over recent years, be it earthquakes like in L'Aquila (Italy 2009) and Izmir (Turkey 1999), Haiti (2010) or the series of massive forest fires in southern Greece and Russia. During those events the crisis response forces gathered crucial information through their work on the best/most adapted practices. In many cases, e.g. forest fires in southern Europe the responders are confronted with recurrent issues encountered previously during a similar situation by other responders. The existing knowledge of EU responders should therefore be gathered and evaluated through an exchange of information, thus creating a "lessons learned database". This would in turn serve for the better preparedness and effective response to the future disasters and improve the capability to restore activity after a crisis situation.

**Objective:**

- As a first step the knowledge acquired by crisis management responders would be gathered, categorised and analysed through consultation with major stakeholders. The methodology should aim for a holistic approach (i.e. including all phases of a crisis, improving the interoperability between first responders and their equipment, the decision making process, identification of victims/people, etc); it could be done through the organisation of workshop(s), conference(s) and/or table-top exercise(s).
- The results of this exercise should then be evaluated involving the main stakeholders on Crisis Management with a focus on the end users. The results should be presented in the form of a "living document" which would be revised on a regular basis.

The learning process itself (from lessons identified to lessons implemented), dissemination means (such as training) have to be investigated. The action should also lead to recommendations for further related research activities. A significant involvement of responders' organisations is essential.

**Funding schemes:** Coordination and Support Action

**Expected impact**: The action should increase the preparedness of the responders, crisis managers and decision makers and provide them with a set of guidelines on the best ways and means for different crisis situations.

## ***Area: 10.4.3 Recovery***

### *Topic SEC-2012.4.3-1 Next generation damage and post-crisis needs assessment tool for reconstruction and recovery planning - Capability Project*

**Description of topic:**
Complex crises situations, wide regions affected operational areas potentially worldwide and growing needs for longer-lasting operations pose specific demands on the reconstruction and recovery planning capabilities of relief forces.

**Objective:**

- The research project should enhance present capabilities by developing a next generation post-crisis needs assessment tool for reconstruction and recovery planning, including structural damage assessment (buildings, bridges, dams) and related data integration and analysis. It should undertake an analysis of the state-of-the-art assessment tools, working out current shortfalls and misfits to be addressed by the project work approach. Aspects to be covered are, among others, reduced time for and continuous updating of damage and needs assessment, recording, storing and presenting identified needs, allowing for collaborative work including mobile/portable assets and the integration of earth observation data, support to improve accountability of humanitarian aid contributions, specific demands for recovery of CBRN incidents.

- The performance of current damage and post-crisis needs assessment tools need to be improved particularly in terms of time required for the assessments, a continuous updating process and international interoperability. Users of these tools are predominantly public and non-profit relief organisations, including NGOs, as well as the EC itself and also UN organisations, thus calling for research at the EU level.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** This project aims at improving reconstruction and recovery planning capabilities of relief units by providing them with technologically improved, faster and more interoperable assessments tools as available today. It is assumed that projects of this kind particularly will deliver new or improved capabilities for users, less aiming at strengthening industrial competitiveness.

***Area: 10.4.4 CBRN Response***

For this area of the Work Programme attention is being drawn to related activities of the European Defence Agency (EDA). For further information see the website of EDA (www.eda.eu).

### *Topic 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 - Coordination and Support Action*

**Description of topic:**
The overall objective of this feasibility study is to provide an evidence based assessment, (including scope, feasibility, operational procedures, costs of building-up and maintenance) of mobile laboratories/structures, equipments and functions to support rapid assessment of threats caused by chemical, biological, radiological and nuclear agents (CBRN related events), with a cross-border or international impact. It should preferably be built on existing EU capacities and expertise. Such Mobile Laboratories/Structures, Equipments and Functions should be made rapidly available (within hours/days) and deployable within and outside the EU. The study should preferably not exceed 1 or 2 years.

The added value of such mobile tools in the context of the EU policy should be carefully examined, including the synergy generated by these tools within the context of other similar EU initiatives currently funded in the specific CBRN sectors for which other Commission

DGs, Services and EU Bodies are responsible (e.g. DG ENTR, DG RTD, DG SANCO, DG HOME, JRC, DG ECHO, DG DEVCO, European External Action Service etc.).

Proposers for this topic should look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Coordination and Support Action (coordination action)

**Expected impact:** This study will provide an evidence-based assessment for the future development of CBRN Mobile Laboratories or Structures, Equipments and Functions. This will reinforce the EU CBRN capacity to react rapidly (within hours/days) and can be deployed within and outside the EU upon request in crisis areas.

### *Topic SEC-2012.4.4-2 Means of decontamination of large groups, urban/wide areas and large, complex and/or sensitive objects - Capability Project*

**Description of topic:**
As underlined in the EU CBRN action plan, further analysis is required to ensure that sufficient capabilities are available through the Community Civil Protection Mechanism in case of need. The research project should look specifically into solutions for the improvement of fast, efficient and environmentally friendly decontamination measures in case of CBRN incidents in public areas and critical infrastructures and subsequent launching of appropriate response as a further way of enhancing European resilience against CBRN emergencies. This should also include release of toxic substances from industrial plants. The decontaminants and applications should have no impact on the population and should also be usable for first time responders. The solutions proposed should facilitate reliable and efficient decontamination measures to medicate the population after incidents.

As underlined in the ESRIF report and in the EU CBRN action plan, further analysis is required to ensure that sufficient capabilities are available in the EU in case of need. The research project should look specially into solutions for the improvement of fast, efficient and environmentally friendly decontamination measures in case of CBRN incidents in public areas and critical infrastructures and subsequent launching of appropriate response as a further way of enhancing European resilience against CBRN emergencies. The project should give clear guidance for decontamination requirements based on the notion ‘how clean is clean’. Possible end users are first responders like fire fighters and rescue services, national and local authorities, hospitals, airports, etc. Due to the psychological impact of mass contamination incidents on civil society the foreseen decontamination means must be accompanied from the start by a broader “societal aspect” approach necessary to assure the societal acceptance of solutions produced by the project.

Current decontamination materials and methods used by specialised civil (e.g. fire fighters, civil protection units) and military decontamination units are particularly suitable for limited decontamination activities, e.g. groups of persons, vehicles, buildings, but lack of a fast treatment for larger areas or larger quantities of people. Furthermore, current decontamination systems have limitations, do not fully neutralize all agents, and are not completely safe and are not appropriate for sensitive equipment (i.e. computers, radio links etc). Strong neutralizers tend to destroy parts of the items decontaminated, including forensic evidence. Some decontaminants have shelf-life or storage issues, some are flammable, and most are not

friendly to the environment and health, which need to be improved by research on novel or alternative materials and methods for an appropriate usability in public areas.

This project will make available new or improved technology able to decontaminate public areas (e.g. subway stations, railway stations, etc) and critical infrastructures (e.g. command centres, hospitals, airports, local authorities) in a more efficient way. It will therefore contribute to a fast treatment of larger quantities of people after dissemination of CBRN agents. Further the project will ensure that critical infrastructures will be operational again in due time after CBRN incidents.

This project is dedicated to deliver new (alternative) or improved decontamination materials and methods, i.e. industrial products. While the market for such decontamination technologies is rather a specialised and limited one, it is expected that economies of scale could be achieved by delivering a European solution, overcoming fragmented national markets and helping to maintain global competitiveness of the herein specialised European companies, predominantly SMEs. The expected research solutions should also provide a distinct cost reduction compared to contemporary military decontamination methods.

Given the cross-cutting character of CBRN, linkages with other ongoing or completed Research activities and studies (across all FP7 Themes and other national or European funding schemes, etc.) should be carefully considered to ensure complementarities, integration and avoid duplications

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** This project will make available a new or improved technology able to decontaminate large numbers of people in public areas (eg. subway stations, railway stations) and critical infrastructures (e.g. command centres, hospitals, airports, local authorities) in a safer and faster way. It will therefore contribute for a fast treatment of larger quantities of people after dissemination of CBRN agents. Further the project will ensure that critical infrastructures will be operational in due time after CBRN incidents. Potential users of the expected developments will be various, public and private: e.g. fire departments, first time responders, hospitals, command centres, airports, local authorities, etc.

### *Topic SEC-2012.4.4-3 Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination - Integration Project*

**Description of topic:**
Research on traceability and monitoring of a large number of people in case of a massive CBRN (Chemical, Biological, Radiological or Nuclear) contamination is needed in order to differentiate between contaminated or not contaminated persons on-site or in hospital zones.

The objective of this project is to integrate existing tools and procedures along with the development of novel solutions in order to:

- Rapidly determine if the person is contaminated or not (by a Chemical, Biological or Radiological contaminant).
- Rapidly determine the level of contamination / exposure (including making use of point of care diagnostic tests).
- Establish a decontamination / treatment / medical follow up based on the level of contamination / exposure.

- Ensure the tools and procedures fit in overarching search & rescue systems.
- Establish guidelines for hospitalisation and admission to intensive care units (or other specific units) based on the contamination evaluation.

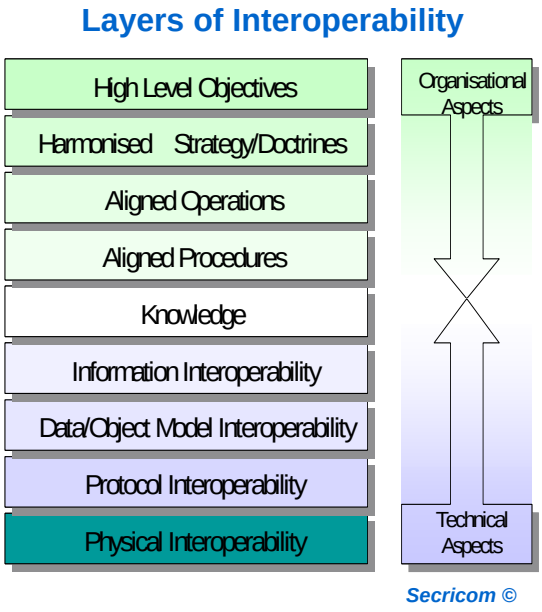
The Ethical implications and social acceptance of the proposed solution has to be studied.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** Breakthrough on detection and monitoring capabilities to the benefit of first responders, civil protection and public health services. In addition, a new integrated, interoperable and centralised system approach involving all stakeholders in case of a mass contamination.

## *Activity: 10.5 Improving security systems integration, interconnectivity and interoperability*

Actions in this activity related to intelligence, information gathering and civil security will enable and/or contribute to the performance of technology required for building up the above listed capabilities, thus focusing on cross-cutting issues such as: enhancing the interoperability and intercommunication of systems, equipment, services and processes, including law enforcement, fire fighting, civil defence and medical information infrastructures, while ensuring their reliability, protection of confidentiality and integrity of information, traceability of all transactions and their processing, etc. Activities will also address standardisation and training matters (including such with respect to cultural, human and organisational interoperability).




This mission area seeks research that takes an outcome-oriented perspective, developing approaches (including methodologies that solve interoperability constraints) to achieve practical interoperability in both the short and longer term, while ensuring the reliability, protection of confidentiality and integrity of information. The focus is on the holistic aspects of interoperability, especially where solutions cut across the other Activity Areas. The relationship between end-user's processes and training with technological issues is expected to be an important element in this Activity. It is recognised that interoperability in the practical context of different organisations and nations is even more about processes than about technology. It is expected that actions in this area will involve research into the interaction between these technological and organisational factors.

Achieving interoperability between information and command functions is a high priority area, but achieving interoperability for other equipment that is deployed in security incidents is also within the scope.

This activity is divided in four areas: **Information Management; Secure Communications; Interoperability; and Standardisation.**

***Area: 10.5.1 Information Management***

No specific topic for this area has been planned for this call.

***Area: 10.5.2 Secure Communications***

### *Topic SEC-2012.5.2-1 Preparation of the next generation of PPDR communication network - Capability Project*

**Description of topic:**
PPDR (public protection and disaster relief) communications systems play a vital role in all security operations and involve a significant national investment. Existing and planned TETRA and TETRAPOL networks provide a secure and resilient mobile voice and data infrastructure with limited features matched to the special requirements of PPDR, including broadcast, dynamic secure groups, push to talk, call priority and secure roaming. Elements of the investment have a life of 20-30 years, however the growing demand for high-speed data communication means that the current system capacity will be exceeded, requiring an upgrade or replacement to the system at some later date. This reality will raise challenging funding issues into the future.

This topic seeks research to inform the medium/long term evolution of PPDR networks, including the overall architecture, matching radio communication platforms to type of operation, development of PPDR standards, use of commercial standards, use of services provided by commercial operators, security and privacy, interoperability within and between nations, and frequency allocation issues. The research should set out potential options, the economic implications and possible migration paths from the current and planned PPDR provision. Architectural solutions can range from complete replacement of PPDR systems, evolution of existing networks through upgrades, overlay of additional networks, for example based on GSM/LTE, partial or full use of commercial operators networks (also Mobile Virtual Network Operator (MVNO)), or some combination of these approaches. The proposers should assess some technological issues as well as economical issues in view of the replacement of PPDR network in the future.

Proposers should also establish some basic data which are still missing related to police forces and first responders like identification of organisation(s) in each members states, number of people involved in each organisation (with and without operational and in the field wireless communication needs; to identify and to count the national events, national cross organisation events, cross border events, external EU event, in short to build a strong statistical base in order to help to build business cases.

Proposers should also investigate how to port existing TETRA/TETRAPOL functionalities required by police forces and first responders like, "push to talk" function, "group call"

function, EU wide group dynamic management; and high priority service and quality of service to another type of network.

Proposers should also study the migration costs, training costs, etc taking into account the time frame of such an evolution and the actual "PPDR communication status" of the Member States.

It is expected that another element of the research will be consideration of future communication demands on PPDR, taking into account the current levels of use and proposing plausible scenarios for growth and adoption of new services over the coming 10-20 years. Factors that might be considered could include changes in PPDR operators processes and behaviours as PPDR networks provide more services, the extent to which video data will be used, increasing database access, deployment of sensors that depend upon communications. If needed, particular attention should be placed on future frequency spectrum requirements. This analysis should be used to develop indicative business cases for options that are proposed. Any near term decisions that could facilitate or pre-empt future options should be highlighted.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Provision of statistical figures, definition of architectural options for future PPDR evolution, related to analysis of future demand, to help political and procurement decisions to be taken in the next 5 to 10 years. The project will also provide insight to equipment and network providers of the potential procurement paths that might be implemented, helping in research and product development planning to meet future market needs.

***Area: 10.5.3 Interoperability***

## *Topic SEC-2012.5.3-1 Embedded protection of security systems and anti-tampering technologies - Capability Project*

**Description of topic:**
Expertise and means of adversary organisations (for instance criminal organisation) are increasing rapidly, especially when high value returns could be expected. It is necessary to develop new technologies to ensure the integrity and confidentiality of data stored inside all sorts of devices, so that information will be safe even when the device is intercepted/stolen. It is also essential to protect equipment against attacks that could grant unauthorized and/or criminal access to the systems to which they may belong.

Many critical applications are based on security solutions/functionalities which rely on high level security hardware and anti-tampering technologies (for example smart card hardware, smart card composite products, TPMs used in trusted computing, digital tachographs, Host Security Modules, police communication systems, etc.). Much work has already been undertaken to try to overcome the limitations of some hardware solutions (like side channel analysis) quite often limiting itself only to the chip and with a limited view on the needed security evaluation (likely based on the Common Criteria and its Mutual Recognition Agreement scheme) and potential accreditation based on these evaluations.

The task is to complement the work done at chip level by adding new technologies (like anti-tampering) for electronic assembly and packaging and to propose generic protection profiles up to the highest possible assurance level, while meeting the need to protect against the highest conceivable level of attack, (like for instance: AVA_VAN.5 as defined by common criteria (CC)). In addition, designing tools, operating systems, and manufacturing process should be developed in such a way as to allow high security for the final product.

Development of these technologies should be compatible both with the constraints on mass-production costs and the highest security standards.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** Obtain the control and a first level of accreditation of these various technologies and of their developers to make sure that high level assurance security solutions will be kept as a competitive advantage for the security industry and available for high security demanding end-users making sure that user's requirements in various high security applications are given a voice in the project.

### *Topic SEC-2012.5.3-2 Establishment of a first responders platform for interoperability - Coordination and Support Action*

**Description of topic:**
The task is to establish an End Users Forum in order to stimulate the cooperation between providers and users (police, fire brigades, emergency services…) at each level of interoperability as presented in the figure above,

- for the use of public safety communication and information management systems to detect gaps and to ensure that the new technologies and tools to be developed fit their needs;
- for users requirements to be collected, assessed, compiled, updated, quantified and made available at EU level on a regular basis;
- to avoid shortfalls by analysing organisational issues, policies and behaviours issues which may lead to obstacles to interoperability.
- to list available standards at each level from highest organisational levels operational processes and policies, as well as technology level and to allow for convergence across Europe.

**Funding schemes:** Coordination and Support Action

**Expected impact:** To involve the end users (police, fire brigades, emergency services, etc.) in the security research projects in a more systematic manner ensuring that research results match their needs, thus improving the interoperability from the lower technical level to the upper organisational level for all types of safety and security missions (large scale and/or daily/ordinary missions as well as local or cross-border missions). To create a global source of information and to support a forum for exchange of information and procedures for all user organisations allowing innovation from one organisation to benefit others.

### *Topic SEC-2012.5.3-3 Establishment of a interoperability platform/centre for testing and validating security innovations - Network of Excellence*

**Description of topic:**
The task is to create a design process and methodology for testing and validation of security innovations in order to create shared platforms/centres for selected segments of the security market. These platforms/centres have to allow end-users to evaluate products, services and systems in a realistic environment and to allow manufacturers to demonstrate the capabilities of their products, services and systems to the end-users, and their interoperability with other tools.

These platforms/centres should provide a development and integration infrastructure in a real working environment or in a simulated environment corresponding to existing or under development standards. The infrastructure should be able to integrate the necessary components and modules to test and to evaluate existing and new solutions. It should be adaptable to include other modules during the full time-life of the platform/centre.

The platforms/centres should offer services for evaluation and a test bench open to end-users and suppliers, to allow them to demonstrate and test products, services and systems in the most realistic environment. It should prepare itself for self sustainability after the initial funding period from the Commission. It should prepare and publish equitable rules for accessing the platform and using the infrastructure, giving full attention to the IPR attached to the tested components.

**Funding schemes:** Network of Excellence

**Expected impact:**
- Improvement of time-to-market in the field of security, by setting up standards for tool integrations and associated methods,
- Better consistency between European tools, resulting in an improvement in communication between European services and end-users of security innovations,
- Coordination of relevant institutions or authorities (as appropriate), acting as certifiers (testing & validation) or procurers (procurement) of new security products, services and systems ,
- Provide the necessary support to suppliers to develop and integrate complementary, innovative technologies and solutions and allow them to benchmark their products and services against the state-of-the-art and standard and
- Feed standardization activities in order to contribute to the creation of a more harmonized market at EU level.

### *Topic SEC-2012.5.3-4 Global solution for interoperability between first responder communication systems - Integration Project*

**Description of topic:**
PPDR (public protection and disaster relief) communications systems play a vital role in all security operations and involve a significant national investment. Since the last 15 years the majority of the member states have undertaken intensive efforts to upgrade their scattered PPDR radio networks to nation-wide digital radio networks. These existing or planned digital radio networks, based on the TETRA standard or the TETRAPOL technology, comply with

the demanding and specific requirements of the PPDR services in voice and short data transmissions, like the ability to make group calls simply by pushing the radio PTT (Push-To-Talk) button.

Unfortunately, until now, the existing national efficient interoperability stops at the borders: the roaming capability (migration to other countries) which is available for the common European citizen thanks to the GSM/3G technology (point-to-point calls), is not available, in both existing technologies, for the PPDR community to save lives and reduce crimes effects.

It has been recognised by the *Council Recommendation on improving radio communication between operational units in cross-border areas* of the 4-5 June 2009 that interoperability between communications systems used by different first responder organisations is currently a key issue for the success of the cooperation within the EU, and requests the development of TETRA-TETRA and TETRA-TETRAPOL Inter System Interfaces (ISI), allowing PPDR services to roam with their own equipment from one country to another one. Moreover, the Recommendation encourages the implementation of interim solutions, like interconnecting solutions (back-to-back relays or more sophisticated gateways), to ensure some minimal cooperation, waiting for the ISI (roaming capability) that is the only technical solution enabling the first responders to fulfil their international missions resulting from the existing international treaties and covenants.

This topic aims to create and demonstrate the development of new - and integration of existing - solutions into a common set of Inter System Interfaces (ISI) prototypes, directly compatible with the existing European nation-wide PPDR radio networks types, in combination of a bi-technology (TETRA and TETRAPOL) radio terminal concept. The ISI prototype functionalities should at least include, voice and short data, international group calls and individual calls, as well as the authentication of the radios working abroad. The security, the privacy and the integrity of the existing systems will be maintained while sharing the needed data for interoperability. The results will be properly disseminated.

The topic aims besides to develop the human and organisational aspects that are associated with the technical solution. Therefore, taking into account the user best practices, the existing legal potentialities and the roaming technical capability, an operational jointly agreed procedures framework will be realised, leading to a standardised functional radio model for international PPDR operations.

The global (technical and organisational) solution performance should be tested on the field by an international panel of multidisciplinary PPDR services, following legally and operationally realistic and varied scenarios. The demonstration should involve at least - a test or a life version of - the main four existing nation-wide PPDR radio networks types.

The feasibility to make gradually interoperate the existing PPDR networks by using a scalable set of ISI systems will be studied using a strong statistical base concerning the international events and operations in order to propose a realistic general design.

**Funding schemes:** Collaborative Project (large scale integrating project)

**Expected impact:** The development of the full compatible set of ISI prototypes is expected to lower the production costs of these devices allowing, for the first time in the TETRA and TETRAPOL history, the formation of a business model for implementing the roaming

between all the European countries, and a unique opportunity, for the member states, to make their national PPDR services efficiently cooperate together during the life cycle of their current systems (from 2016 to at last 2025). The project will also provide the multidisciplinary operational framework for an international standardised use of the roaming capability as well as a clear idea of the international occurrences that will take a direct benefit of the project.

***Area: 10.5.4 Standardisation***

No specific topic for this area has been planned for this call.

## *Activity: 10.6 Security and society*

Actions in this activity are of a cross-cutting nature and should be conducted by interacting between natural sciences, technology and other sciences, in particular political, social and human sciences. The focus will be on targeted cultural and socio-economic, as well as systemic risk analyses, scenario building and other research activities related to subjects such as: Security as an evolving concept (comprehensive analyses of security-related needs, in order to define the main functional requirements to address the fluctuating security landscape); interdependencies, vulnerabilities due to disasters and new threats (e.g. in the field of terrorism and organised crime); the attitude of citizens in crisis situations (e.g. perception of terrorism and crime, behaviour of crowds, public understanding of civil rights and socio-cultural forms of protection and acceptance of security (and safety) controls); preparedness and readiness of the citizen in case of terrorist attacks; issues related to communication between authorities and citizens in crisis situations; raising public awareness for threats; citizens' guidance on the internal security advisory and assistance systems in the Member States and at EU level; behavioural, psychological and other relevant analyses of terrorist offenders; ethical issues with respect to personal data protection and integrity of information. Research will also be directed into developing statistical indicators on crime to permit assessments of changes in criminality.

Security, whilst very important, is just one of the societal values in Europe which must be balanced against others. It is a tool in support of freedom and can only be achieved within the rule of law. The EU Member States have all signed up to the European Convention on Human Rights and the EU's Charter of Fundamental Rights has become legally binding. The EU and its Member States are bound to respect and to promote human dignity, freedom, democracy, equality, the rule of law and protection of fundamental rights (which include both the right to privacy and the right to security).

In this activity, the objective is to carry out research into all those political, social and human factors that influence European security solutions and related new technologies, and to specify how the proposed security solutions must be adaptable to diverse cultural and institutional settings.

Actions in this activity will provide improved insight and advice for security policy makers, security research programme makers and (mission oriented) security research performers (in some cases, acting as "Think Tanks"). They aim to obtain a broad and well-based understanding of the public administrative, cultural and societal frameworks in which security

enhancing policy measures, including in particular security research, take place. In particular they effectuate in-depth understanding of the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. The outcome of the research together with appropriate dissemination strategies contribute to the effective and efficient planning and designing of future security research programmes and actions as well as to policies, programmes and initiatives which enhance the security of the European citizens.

As this activity takes a threat and incident related approach only, it is complementary to the more general approach of Theme 8 *Socio-Economic Sciences and the Humanities (SSH),* of the Cooperation Programme, as well as to the *Science and Society* area of the Capacities Programme. The objective of the Socio-Economic Sciences and the Humanities is to generate in-depth, shared understanding of complex and interrelated socio-economic challenges in Europe. Human security and international security are addressed as one of these challenges and set in the general landscape.

Science and Society has the objective to stimulate, with a view to building an open, effective and democratic European knowledge-based society, the harmonious integration of scientific and technological endeavour, and associated research policies in the European social web by encouraging pan-European reflection and debate on science and technology and their relationship with the whole spectrum of society and culture. In that context, ethics in science and technology is addressed.

The security and society activity in the Security theme is targeted towards security challenges and addresses immediate and medium term issues.

Coordination between these activities takes place on a regular basis in order to ensure synergy and take advantage of the available knowledge.

This activity is divided among five areas: **Citizens, media and security; Organisational structure and cultures of public users; Foresight, scenarios and security as an evolving concept; Security economics; Ethics and Justice**.

***Area: 10.6.1 Citizens, media and security***

Research in this area will ensure that selected policies and technologies are responsive to the needs of the citizens, and that they create security approaches that are rooted and acceptable by society and citizens, with differing cultural backgrounds. It will also support political accountability and democratic control aspects of public services within the security arena.

### *Topic SEC-2012.6.1-1 Methodologies to assess the effectiveness of measures addressing violent radicalisation - Capability Project or Coordination and Support Action*

**Description of topic:**
This topic aims at developing a viable, practical approach and methodology to facilitate the measuring of the effectiveness of measures and policy responses to address the phenomenon of violent radicalisation.

Since the adoption of the 2005 EU Strategy for Combating Radicalisation and Recruitment there has been no thorough evaluation of the measures and policy responses mostly due to the lack of appropriate evaluation methodologies.

Interventions can be different in nature and approach, and may therefore need also custom-tailored evaluation. There is a need for guidance in and an overarching approach to carrying out this process, which start at the moment a possible radicalisation issue is identified, and interventions are developed and implemented.

Proposals should take into consideration previous (empirical) work concerning interventions and their effectiveness, as well as work concerning measuring effectiveness in general. The resulting approach should be applicable at both the strategic and operational levels.

The proposal should address not only the process of measuring effectiveness, but also how best to implement knowledge management of lessons learned and best practice.

Given the transnational nature of the phenomenon and in order to avoid duplications of efforts among the EU Member and Associated States, research at the European level is appropriate. Though the ultimate goal is to improve society's ability to address threats to public security posed by violent radicalisation, proposals should take into account any potential negative societal impact in terms of violations of ethics, civil liberties or human rights.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action (coordination action)

**Expected impact:** This research should allow for a more standardised modus operandi for measuring effectiveness and evaluating interventions. Thus it should make possible the selection and implementation of more appropriate response measures, and the designing of better and more focused policy, while respecting civil liberties and human rights.

### *Topic SEC-2012.6.1-2 Tools and methodologies, definitions and strategies for privacy by design for surveillance technologies, including ICT systems - Capability Project or Coordination and Support Action*

**Description of topic:**
The balancing between increasing security and enhancing security measures on the one hand and preserving the fundamental rights of citizens for privacy, justice and freedom on the other, should be the driving force for any investment in security.

Due to the increasing pace of technological development, citizens experience a sense of opaqueness and loss-of-control with regard to the capabilities of new technologies and systems. Moreover, the concept of private (vs public) is evolving over time, and there is a different apprehension of this concept depending on the individual situation (sociological dimension), on cultural and surrounding environmental factors (anthropological dimension) and on the legal situation (legal dimension).A definition of the concept of privacy versus public is therefore needed in order to better understand as to when (from a sociological, anthropological, and legal point of view) a certain space or situation are considered private (versus public).

Based on a definition of the notion "private vs public", the aim is then to develop tools, methodologies and strategies to support the application of knowledge about privacy during the design phase of technologies and systems.

Privacy is a property that has to be designed into surveillance technologies and systems; it does not emerge by itself. As such, the concept of privacy by design - including data protection by design - should be an inseparable part of the wider concept of security by design.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

**Expected impact:** A technology that is developed on the basis of privacy by design, for which a better understanding of the evolving concept and notion of public and private is needed, would make it more acceptable to citizens and thus enhance their trust in new surveillance technologies and systems.

### *Topic SEC-2012.6.1-3 Use of new communication/social media in crisis situations - Capability Project or Coordination and Support Action*

**Description of topic:**
The aim is to explore the rapidly expanding new communication media (smart phones, mobile phone applications and functionality, Twitter, social networking sites - such as Facebook, etc) in order to give guidelines for the most efficient and effective ways to enable and encourage users of these new media to contribute to the security of the citizen in crisis situations and for search and rescue actions.

This topic would not only examine the potential to establish better communications between the police/law enforcement agencies/first responders and among the public, but should also investigate opportunities stemming out of the proliferation of hi-tech and mobile devices to gather local information (e.g. location, sent messages, etc). The topic also includes communications in both directions. Social media have proven to have high impact when it comes to citizens sharing their observations, opinions and emotions. The topic further examines the role of the public as a participant in the process of emergency communication and in this context the ethical dimension should be taken into account.

Opportunities stemming out of the application of new technological opportunities such as crowd mapping, visualisation analytics, remote sensing, processing real time image of the local situation, information mining, etc should be taken into account.

The proposal should complement on-going research in this area and look for an enhanced international cooperation as described in Part I of the Work Programme.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

**Expected impact:**
- More rapid response to the benefit of the ordinary citizen.

- Better linkages between prevention, detection, reporting, and rescue.
- More effective and efficient police and law enforcement agencies as well as for first responders and medical personnel.

***Area: 10.6.2 Organisational requirements for interoperability of public users***

An objective European joint security capability to handle security matters has to be based upon the resources and mandates of the Member States and Associated Countries. The distinct national systems must be interoperable, scalable and allow for mobility where appropriate. Research under this area will look at the organisational structures, behavioural and cultural issues of end user organisations in order to ensure applicability, user friendliness and affordability of security technologies and solutions.

No specific topic for this area has been planned for this call.

***Area: 10.6.3 Foresight, scenarios and security as an evolving concept***

Research under this area will improve our understanding of novel threats as well as technological opportunities and emerging security related ethical, cultural and organisational challenges. It will help authorities to assess investment alternatives for prevention, early warning or preparedness and to make the appropriate choices in addressing threats to public security that achieve social cohesion and fully respect fundamental rights, in particular the protection of personal data.

### *Topic 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 - Capability Project*

**Description of topic:**

The aim is to conduct research into technologically-/actor-driven systems and tools which support environmental scanning to enable the rapid identification and qualification of new Organised Crime (OC) threats within the policing and law enforcement environment.

Strategic Early Warning Systems increasingly use environmental scanning techniques to systematically monitor the external environment for the detection of “weak signals” of upcoming opportunities and threats.

The detection of those signals enables the strategic decision makers within the organisation (or externals) to counterbalance detected upcoming threats before they materialise.

Using concepts such as ‘Criminal Hubs’, ‘Indicators’ for OC groups and ‘Facilitating Factors’ for OC activities, it is possible to map changes within the OC situations that impact the security of the European Union (EU) Member States.

The EU and National Policy Cycles have foreseen continuous environmental scanning functions performed by policing bodies and/or criminological institutes. This function is designed to scan the environment to feed new and emerging threats into the serious and organised crime threat assessment processes.

Research is required to identify a combination of technological resources and human actors that serves to improve the process of detecting and selecting new OC threats that warrant EU-level analysis and EU-wide responses.

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:**

- Demonstrating the feasibility and testing new systems.
- Increasing the effectiveness of the National Police Forces, criminological institutes and private businesses.
- Providing more effective information into foresight to fight against terrorism, drug trafficking and all sorts of organised crime.
- Providing a better understanding of the new and upcoming technologies and trends, leading to the strategic planning into security issues of all stakeholders.

### *Topic SEC-2012.6.3-2 Criteria for assessing and mainstreaming societal impacts of EU security research activities - Coordination and Support Action*[41]

**Description of topic:**
The aim is to provide tools, such as guidelines and recommendations, on how to assess and mainstream societal impacts of EU security research activities in the future.

The work should include an overview of the current state of the art on societal security, including present good practices. The work could be done by desk research and workshops. It should also aim at creating a pool of expert in this field, which could provide assistance to the Commission in implementing the recommendations. The outcome should include a roadmap on how to implement these aspects in the next framework programme for research and innovation.

**Funding schemes:** Coordination and Support Action

**Expected impact:** To ensure a better integration of the societal dimension of security research activities already from the start of new EU projects, activities and programmes.

### ***Area: 10.6.4 Security economics***

Research should include all economic impacts of security aspects, investigate the economic causes and consequences of insecurity, and the direct and indirect costs of security policies and how they contribute to or hinder economic growth. Understanding how perceptions, for example fear of terrorism, shape economic behaviour is also important. Evaluating the cost-benefit relationship of security measures, even if difficult to assess, is important. Cost calculations should place specific emphasis on less visible impacts, including increased hidden costs, decreased efficiency and trans-boundary impacts, such as the interaction between security behaviour and economic growth over time. Society needs basic market data to understand the structure, conduct and performance of the security sector. Economic theory

[41] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.

can offer key insights, enabling policy makers to optimise efforts to enhance security and growth.

### *Topic SEC-2012.6.4-1 Fight against corruption - Coordination and Support Action*

**Description of topic:**
Corruption, as defined by the UN and endorsed by the EU, is the "abuse of power for private gain". It is an insidious crime that undermines trust and societal resilience, no country in the world being immune to it. Its consequences can be far reaching and corrupt decisions may negatively impact on future generations. Corruption is as well an obstacle to development and the EC is taking a number of measures to tackle graft in the countries which receive EC technical assistance and aid. By mainstreaming anti-corruption measures the EC seeks to build institutional capacity and thus, ideally, reduce fiduciary risks or misuse of funds.

Corruption cannot be addressed in isolation but rather as part of the overall support to democratic governance reform processes. Taking into account the international and European context (e.g. UN Convention against Corruption, Stockholm Programme), the aim is to develop tools and methods to facilitate the prevention, the detection and the repression of corruption. It will also include networking activities, exchange of best practices and dissemination activities to and between the stakeholders. Legal aspects (e.g. restriction to exchange of information between national authorities), within the EU or at international level will have to be addressed. Targeted training activities could be envisaged.

The activities should complement on-going and planned research in this area, for instance with the SSH theme.

**Funding schemes:** Coordination and Support Action

**Expected impact:** To provide law enforcement agencies with better tools and methods to fight more efficiently corruption in Europe and internationally.

### ***Area: 10.6.5 Ethics and Justice***

Security technologies and policies raise various ethical and legal concerns, which influence public support and acceptance. Research under this area will address the privacy, data protection and human rights issues as well as acceptability, ethical and prioritisation issues, while taking into account a variety of approaches to ethical, social and legal questions based on divergent ethical, religious, historical and philosophical backgrounds. Aspects of social exclusion, lack of social cohesion that may lead leading to the formation of areas of insecurity within Europe may also be considered, as well as aspects of the European Neighbourhood Policy relevant to security. This will contribute to the general discussion and help both security solution suppliers as well as end users to make better decisions when selecting and applying security technologies and solutions.

### *Topic SEC-2012.6.5-1 Legitimacy and effectiveness of legal measures against security threats - Capability Project or Coordination and Support Action*

**Description of topic:**

Today, the discourse on counterterrorism is a lively field, covering a wide array of international and national political initiatives. In Europe, the controversy focuses on the regulatory scheme with which the EU attempts to address seemingly new forms of terrorism.

Anti-terrorism policies respond to real threats, but also to perceived needs for action. New legislation purporting to combat terrorism is frequently legitimated by a reference to the improvement of security for the citizen. However, it is often not clear, from a sociological perspective, whether the legislation in question is effective at all, calling, from a legal point of view, into question the proportionality of the given measure.

Moreover, new counter-terrorism policies have led to legislation that often departs from traditional patterns, such as the clear distinction between prevention and punishment. It is very difficult to define in precise legal terms when a preventive measure based on an actuarial risk-assessment is legally required or permitted. If the risk is considered complex and the potential damage substantial, the line between legitimate intervention and the illegitimate intrusion in the citizens' rights are not easy to draw.

- The aim is to integrate sociological and legal research on the legitimacy and efficiency of counter-terrorism measures on a European level and on the level of the Member states with research in the field of security studies that often neglects social and legal aspects of counter-terrorism measures. The following questions should be examined: Comparatively, how have European anti-terrorism measures been transposed into legislation in the Member States? Sociologically, what is the state of art in determining the effectiveness of anti-terrorism legislation, and how do selected legal instruments perform when analyzed as to their effectiveness and impact? Normatively, what are the consequences when assessing the legitimacy of the various legal measures which may intrude into the lives of the citizens?

**Funding schemes:** Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

**Expected impact:** Provide feedback to (administrative and legislative) experts about state-of-the-art research on the effectiveness of anti-terrorism legislation. Provide examples of best-practice and failures of implementation. Make an empirically informed contribution to the ongoing debate on the relationship between security and freedom on the European level.

## *Activity: 10.7 Security research coordination and structuring*

This area provides the platform for activities to coordinate and structure national, European and international security research efforts, to develop synergies between civil, security and defence research as well as to coordinate between the demand and the supply side of security research. Activities will also focus on the improvement of relevant legal conditions and procedures.

The Security theme, aiming at increasing the security for Europe’s citizens and simultaneously improving the global competitiveness of Europe’s industrial base, needs to utilise limited resources in an effective and efficient manner. It is embedded in a fabric of other relevant research work carried out under various other programmes both on the

European level as well as in the Member States and Associated Countries. It can only reach its objective, if its outcome is eventually applied by the relevant end user communities.

It is understood however, that there will be certain areas where coordination and structuring are not sought, or needed, but equally there will be others where coordination and even co-operation would add value.

Actions in this activity will provide deeper insight and wider awareness of the European security related research and industrial landscape and the public environments and frameworks in which stakeholders operate. In particular actions will indicate opportunities and constraints for developing and strengthening a European security related market. Actions will ensure enhanced networking, coordination and co-operation of the Member States and Associated Countries as well as between relevant organisations on the European level. All this which will contribute to the overall impact of the Security theme by making it more effective and efficient, it will raise the innovation level in the security domain and will achieve increasingly harmonised implementation approaches. It will also contribute to the design of future Work Programmes of the Security theme.

This activity is divided in six areas**: ERA-Net, Small and Medium Enterprises; Studies; Other coordination; End users; and Training.**

***Area: 10.7.1 ERA-Net***

No specific topic for this area has been planned for this call.

***Area: 10.7.2 Small and Medium Enterprises***

### *Topic SEC-2012.7.2-1 Open topic for Small and Medium Enterprises: "Advancing contemporary forensic methods and equipment" - Capability Project*

**Description of topic:**
The aim of this topic is to advance contemporary forensic techniques and methods. These developments should take into account the legal constraints to maintain the chain of custody from the field to the court.

One of the objectives of this topic is to encourage Small and Medium Enterprises (SMEs) to become more involved in Security research.

Any advancing contemporary laboratory forensic methods and equipment could be selected and developed by the proposer. Indicative research areas could be for instance:
1) open repository of data stemming from fire/explosion scenes to allow Europe-wide identification and comparison,
2) improve techniques used to authenticate documents and to identify their author,
3) guarantee integrity of digital data within a specific chain of custody,
4) develop microbial ecology to profile soil types and to link them to suspects,
5) develop tools and protocols to deal with radioactive evidence or
6) any other forensic science field.

The proposed research project should complement existing projects/activities in the proposed area.

For each project/consortium, the following recommendations apply:

- an average of 50% of the EU funding should go to eligible SMEs
- small-sized projects are encouraged (up to € 2 million total cost)
- the project duration should be up to 2 years
- small-sized consortium (3-7 partners) and/or an SME coordinator are encouraged
- at least one end-user should be included in the consortium

**Funding schemes:** Collaborative Project (small or medium-scale focused research project)

**Expected impact:** It is expected that the outcome of these projects will be developed, benefit and validated by the forensic community. It is also expected that through this topic SMEs will play a more active role in the development of new innovative technologies or services in the chosen area. A clear potential for exploitation of the results, within EU and world-wide, by the involved SMEs is expected, given also the interest by the EU to contribute to a growing vibrant and globally competitive European security SME sector. A significant and demonstrable impact for end-users is also expected.

***Area: 10.7.3 Studies***

No specific topic for this area has been planned for this call.

***Area: 10.7.4 Other coordination***

### *Topic SEC-2012.7.4-1 Coordination of national research programmes in the area of security research - Coordination and Support Action*

**Description of topic:**
The aim is to ensure effectiveness and efficiency of the Security theme by supporting cooperation and coordination of national and, where appropriate, regional security research activities. The activities can either concentrate on coordination in a specific core area of Security research or cover several areas. As part of the activities a network should be established with competent and politically relevant actors in Member States and Associated countries'. The action should further aim to: a) exchange information on security research issues in their countries and define core areas of common interest in order to prevent duplication and identify synergies, b) develop common strategies and mechanisms in the specific area(s), c) explore and demonstrate coordinated and/or joint activities in the area of Security Research.

**Funding schemes:** Coordination and Support Action

**Expected impact:** Actions will ensure enhances networking, coordination and co-operation of Member States and Associated States as well as between relevant organisations on the European level. The activities should contribute to improving the effectiveness and efficiency of the Security Research theme and achieve more harmonised implementation approaches.

### *Topic SEC-2012.7.4-2 Networking of researchers for a high level multi-organisational and cross-border collaboration - Network of Excellence*

**Description of topic:**
An increasingly large number of experts in Europe work on security research, with knowledge and specialisation in this area. However it is sometimes difficult to find and identify the right expertise at the right location and the right moment. Dedicated training actions in the domain of security are also relatively scarce in Europe. European security research experts are spread over many EU countries, thus stressing the need to create virtual centres of research competence to network all this expertise, to exchange knowledge, develop new ideas and new trends in their respective area.

The topic aims at an integration and reinforcement of existing co-operations and cross-border collaborations, as well as establishing new ones, at high level in the security research domain, and at the same time stimulate appropriate training activities. Researchers and entities (research centres, stakeholders, from both academia and industry, as well as end-users) ready to integrate a part of their research activities should become part of this network. This integration should start around some concrete technical projects and aim for a long lasting cooperation based on a joint programme of work leading to the emergence of a 'virtual research centre' in a specific security domain. This network could focus on specific areas of Security research. Activities on cyber-defence, secured communication or related to the societal dimension of security are strongly encouraged.

**Funding schemes:** Network of Excellence

**Expected impact:** Virtual centre(s) of competence in specific domain of security research should increase the quality and impact of relevant training and research in Europe by bringing together the top specialists and encourage the exchange of knowledge, development of new ideas and new trends in the respective area. By virtue of such a virtual structure the innovation process should be significantly enhanced, to the benefit of the competitiveness of EU security industry and the enhancement of the security of the citizens. The research networks could also be used for providing advice to policy-makers in their respective domain.

## ***Area: 10.7.5 End users***

No specific topic for this area has been planned for this call.

## ***Area: 10.7.6 Training***

No specific topic for this area has been planned for this call.

# III IMPLEMENTATION OF SECURITY RESEARCH CALL 5

**For description of the topics of the call, please refer to section II**

**Call title: FP7-SEC-2012-1**

- **Call identifier**: **FP7-SEC-2012-1**
- **Date of publication**: 20/July/2011[42]
- **Deadline**: 23/November/2011 at 17.00.00, Brussels local time [43]
- **Indicative budget**: Total call budget EUR 241.7 million [44]

  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 | None | |

[42] The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.
[43] The Director-General responsible may delay this deadline by up to two months.
[44] Under the condition that the draft budget for 2012 is adopted without modification by the budgetary authority.

| | | |
|---|---|---|
| Ordinary Crime and Forensic | | |
| 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 against major deliberate, accidental or natural CBRN-related contaminations | CP-FP |
| | 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 tools | CP-CSA |
| 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 | CP-IP |

| | | |
|---|---|---|
| | unpredictable behaviour | |
| | SEC-2012.4.2-3 Post crisis lesson learned exercise | CSA |
| Area: 10.4.3 Recovery | SEC-2012.4.3-1 Next generation damage and post-crisis needs assessment tool for reconstruction and recovery planning | CP-FP |
| Area: 10.4.4 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 Information Management | None | |
| Area: 10.5.2 Secure Communications | SEC-2012.5.2-1 Preparation of the next generation of PPDR communication network | CP-FP |
| Area: 10.5.3 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 Standardisation | None | |
| **Activity: 10.6 Security and society** | | |
| Area: 10.6.1 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 users | None | |
| 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'.

# IV OTHER ACTIONS[45] (not implemented through calls for proposals)

In addition to the above schemes and call for proposals, the following actions will be supported:

- **Call for tender:[46] [47] Civil security R&D in major third countries**

  This action in the third trimester of 2012 aims at studying the civil security R&D programmes in major third countries, such as for example the US, Canada, Russia, Japan, etc., as well as its impact on the security industrial base in these countries.

  Whilst there is a lot of general information available on civil security R&D programmes in major third countries, an in-depth analysis of the differences, as well as of the strong and weak points of these programmes and in particular how these programmes relate to the security industrial base in these countries is missing.

  Such a comparison should allow for useful input in terms of future international security R&D cooperation.

  **Indicative Budget:** up to EUR 1 000 000.

  **Funding scheme:** Coordination and Support Action – public procurement

  **Expected impact:** Actionable recommendations for future international security R&D cooperation

- The use of appointed **independent experts** for the evaluation of proposals, and as independent observers at these evaluation, and where appropriate, for the reviewing of running projects.

  **Indicative Budget**: up to EUR 1 600 000.

  **Funding scheme**: Coordination and Support Action – expert appointment letters

- **Support to workshops, conferences, expert groups, communications activities or studies**

  In addition to calls for proposals, calls for tenders for up to EUR 2 000 000 in 2012 are also expected to be published on specific activities that the security theme will support.

  These include:

[45] In accordance with Articles 14, 17 and 27 of Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013).
[46] Policy related action: the management of any resulting contract(s) will not be externalised to the REA.
[47] Call for tender can also be attributed via a framework contract.

a) Organisation of an annual Security Research event. Four service contracts are planned to be concluded in the second semester of 2012, and existing Framework Contracts will be used for this purpose.

**Indicative Budget**: up to EUR 1 000 000.

**Funding scheme**: Support Action – framework contract

b) Support to workshops, expert groups, communications activities or studies
Workshops are planned to be organised on various topics to involve end-users such as for example on "Logistics and supply chain security", to support an expert group on societal issues, to prepare information and communication material etc.

**Indicative Budget:** up to EUR 1 000 000.

**Funding scheme**: Coordination and Support Action

# V BUDGET

**Theme SECURITY - Indicative budget**

| **Activities** | **2012[48] Budget EUR million[49]** |
|---|---|
| Call FP7-SEC-2012-1 | 241.70 |
| General activities (cf Annex 4) (details below) | 2.48 |
| Other actions:<br>• Expert Evaluators (EUR 1.60 million)<br>• Actions implemented through public procurements, expert groups and grants to identified beneficiaries (EUR 3 million) | 4.60 |
| **Estimated total budget** | **248.78** |

**General activities - indicative budget**

| **Activities** | **2012[50] Budget EUR million** |
|---|---|
| CORDIS | 0.38 |
| ERA-NET<br>- Scheme<br>- Experts | 0.05 |
| EUREKA | 0.02 |
| COST | 2.03 |
| **Total** | **2.48** |

All budgetary figures given in this work programme are indicative. The final budgets may vary following the evaluation of proposals.

The final budget awarded to actions implemented through calls for proposals may vary:

[48] Under the condition that the draft budget for 2012 is adopted without modifications by the budget authority.
[49] The Budget figures given in this table are rounded to two decimals points.
[50] Under the condition that the draft budget for 2012 is adopted without modifications by the budget authority.

- The total 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.

For actions not implemented through calls for proposals:

- The final budgets for evaluation, monitoring and review may vary by up to 20% of the indicated budgets for these actions;
- The final budget awarded for all other actions not implemented through calls for proposals may vary by up to 10% of the indicated budget for these actions.

# VI INDICATIVE PRIORITIES FOR FUTURE CALLS

**Indicative roadmap for future calls**

Security call 6 (FP7-SEC-2013-1) – open 2nd half of 2012

**Indicative approach of call 6**

Demonstration project(s) phase II for "Logistics and supply chain security"
Demonstration project(s) phase II for "Aftermath crisis management"