Cooperation theme 10: Security (9 July 2012)

Caption: Cooperation theme 10 on Security is adopted by the European Commission on 9 July 2012 as part of Work Programme 2013. Its aim is to help develop technologies and knowledge that can increase security for citizens and improve competitiveness for industry. The Security theme involves five sections: the first describes the general context; the second includes all the topics for which proposals will be called in this work programme; the third deals with the practical arrangements related to the calls; the fourth focuses on actions that are not implemented through calls for proposals; and the fifth concerns the indicative budget.

Source: European Commission. Cooperation Theme 10: Security, Work Programme 2013, C (2012) 4536. 09.07.2012, 105 p.

URL: http://www.cvce.eu/obj/cooperation_theme_10_security_9_july_2012-en-c4777366-8ac3-4f82-a25e-9bb1249f2e54.html

Publication date: 02/12/2013

WORK PROGRAMME 2013

COOPERATION

THEME 10

SECURITY

(European Commission C (2012)4536 of 09 July 2012)

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 human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to stimulate the cooperation of providers and users for civil security solutions, improving the competitiveness of the European security industry and delivering 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 Small and Medium Enterprises), enhancing the competitiveness of European industry, closing the gap between research and market, ensuring a better involvement of SMEs, 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 2013 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 in support of delivering 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 two topics on pre-operational validation.

This work programme also contributes to the Innovation Union by identifying and addressing exploitation issues, like capabilities for innovation and dissemination, and by enhancing the

[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

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 online[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 focuses exclusively on civil application.

The Security theme facilitates the co-operation and coordination of various national and international actors 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 September 2006 recommendations of the Commission's *European Security Research Advisory Board (**ESRAB**)*[12], the Security theme addresses four security **mission areas** of high political relevance. It contributes to building up the **capabilities** necessary for safeguarding security in these mission areas by funding the research that will produce **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.

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

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

In September 2007, the *European Security Research and Innovation Forum (**ESRIF**)* was established with 64 high level members, including two representatives of the European

[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.*

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 the Commission welcomed the ESRIF Report[14] and acknowledged its importance in the context of the FP7 Security theme.

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 are key requirements for exploiting 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.

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. This will be done through *adaptation of available technology* in its appropriate societal context 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 the 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

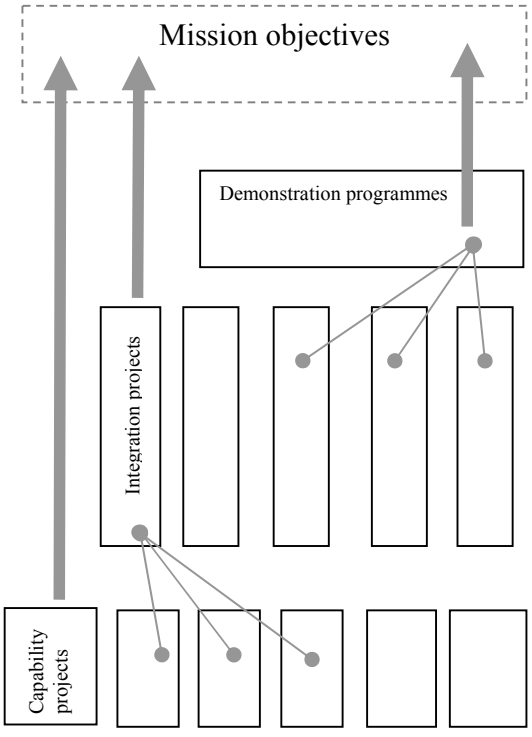


Figure 1: Research routes to meet the Security theme objectives

[13] See www.esrif.eu
[14] COM(2009)691

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:

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)**: the POV differs from and complements the other project types such as CPs, IPs, DPs , 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 be done either via a decentralised network (of national agencies / public bodies) or via a single EU Agency or a combination of 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.

  Funding would be in general for one (or both) of two purposes:
  (i) the *coordination* of relevant institutions or authorities (as appropriate), acting as specifiers and *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). In the case of collaborative projects more than 75% of the EU contribution should be aimed at developing and testing technologies.

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 issues will also be integrated into technology projects.

[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.

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.

  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!

- **Coordination and Support Actions** (CSA) are divided in **Coordinating Actions** and **Supporting 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

[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*

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, **two open topics for SMEs** have 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 high income countries as well as to ICPC[18] countries. The proposal should clearly explain how far the contribution of the international partner(s) is essential in order to allow a better assessment of their potential co-funding. As a specific action, the topic 2.4-1 is 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. For this specific action (topic 2.4-1) an EU financial contribution is foreseen.

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**

[17] http://cordis.europa.eu/fp7/ict/international/st-agreements_en.html
[18] *ICPC: International Co-operation Partner Countries - see Annex 1.*

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 6.

Attention must be given to the **societal impact**[19] of the proposed security solutions. Awareness of the project's contribution to the security of European citizens and 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, proportionality and accountability while displaying awareness of the fact that security risks can be unevenly distributed within and between societies. Proposers should 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 and knowledge 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 persons with disabilities where relevant at all levels in research projects are encouraged, including in evaluation groups etc. On the research output side, awareness of gender-difference is needed in both exposure to security threats and in the impact of security measures.

[19] See separate checklist on how to assess societal impact in Security research projects annexed to the Guide for Applicants.

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*[20] 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 6 (FP7-SEC-2013-1), **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 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*[21], 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.

Modalities of Implementation: The Research Executive Agency

Call for proposals and other actions under this work programme will be implemented by the Research Executive Agency (REA) according to the provisions of the Commission Decision C/2008/3980 of 31/7/2008 "delegating powers to the Research Executive Agency with a view to performance of tasks linked to implementation of the specific Community programmes

[20] *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*

[21] '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.

People, Capacities and Cooperation in the field of research comprising, in particular, implementation of appropriations entered in the Community budget".

II. SECURITY RESEARCH CALL 6 (FP7-SEC-2013-1)

This section describes all the topics for which proposals will be called in this work programme. This concerns only the content of the calls. For the practical modalities related to these calls, please refer to section III 'Implementation of calls'. For actions not implemented through calls for proposals, please refer to section IV 'Other actions'.

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

All seven activity areas, the four mission-oriented and the three cross-cutting areas have topics in the Security call 6. 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, and societal approaches),
- 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 impact projects (with a view at long-term development of groundbreaking new technologies and other solutions).

The topics that are open to the submission of proposals under the Security Research Call 6 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.

Activity 10.1 SECURITY OF CITIZENS

Activities will concentrate on threat aspects of potential incidents of a transnational 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.

Area 10.1.1 Organised crime

Topic SEC-2013.1.1-1 Serious organised economic crime – Integration Project

Description of topic:
Serious organised economic crime is undermining states by reducing their available resources (e.g. reducing tax precepts - for instance TVA fraud counterfeit goods, carburant laundering, arm, drugs, alcohol, tobacco trafficking, etc.) or reducing trust of the citizens (use of false marking of goods, corruption, social fraud) or by directly endangering the functioning of some public services (for instance by stealing copper from energy and railway networks). The objectives of this research are:

- to build an agreed extended European taxonomy and inventory of economic crimes and frauds including the low level or low intensity ones;
- to evaluate their importance both in terms of economic value and loss of state revenue;
- to investigate possibilities for creating a systematic monitoring such activities, including the emergence of new trends and methods and
- to develop a pan European system in order to respond.

New detection solutions and/or methodologies to fighting these crimes/frauds should be developed as an integral part of any proposal.

The proposed project should develop and demonstrate a multi-layered, multi-source pan-European system integrating economic crimes/frauds monitoring systems and new solutions to deter these crimes/frauds. The project should also take into account the legal implications linked to the development of such an EU wide system.

Proposers should take into account other EU and national research projects.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
Increasing awareness of the public at large and of the political personnel on the particular type of crimes/frauds by giving them standardised information both at EU level and each Member State/Associated Country; helping the Law Enforcement Agencies (LEA) and other relevant public authorities doing a better job in fighting these crimes/frauds; increasing the trust of citizens in the proper functioning of states. Proposers are expected to show how the project will strengthen the research base and provide opportunities for new products and services that enhance industry competitiveness.

Topic SEC-2013.1.1-2 “Stronger Identity for EU citizens” – Capability Project

Description of topic:
Identity theft is becoming a major concern not only in the "cyber" world but also in the "real" world. It is a serious crime, often part of organised crime. It covers all forms of identity (civil, financial, medical, social, etc.). The "civil registration" process on which is based our "identity" - which in most European countries was designed under the Napoleonic era - could be improved as well as other identification processes (bank account opening, car registration, etc.) and authentication processes. The weaknesses in these processes make the forging of false documents (paper and/or electronic), notably by using available digital means easier than before.

The research efforts should focus on the protection of individuals and organisations, and, as a minimum, cover the following tasks:

- to build an inventory of the various forms of identity theft in EU Members States/Associated Countries;
- to assess the importance of this threat and its economic impact;
- to develop solutions to prevent or detect identity theft. This can include improved life-long processes, approaches, procedures, methodologies, and technologies against identity theft. These solutions will have to pay a special attention to the respect of privacy and data protection regulations; and
- better services and commercial activity based on the advance made in the area of identity protection.

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

Expected impact:
A common European approach related to identity theft including:

- proposals for harmonised standards/procedures for tackling identity theft in Europe;
- contribution to identity theft legislation/policies in the European Liberty, Security and Justice Framework;
- innovative approaches and solutions to make identity fraud more difficult;
- increasing information awareness amongst citizens and other stakeholders on identity theft and the subsequent identity recovery; and
- better services and commercial activity based on the advance made in the area of identity protection.

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-2013.1.3-1 Inhibiting the use of explosives precursors – Capability Project

Description of topic:
Home made explosives are easy to make from readily available materials used for legitimate purposes in everyday life. Basic chemicals (precursors) for the production of explosives are easily accessible. Normal day-to-day household chemicals can be used to prepare more dangerous compounds. Previous FP7 funded projects have started to work on this issue. However, the list of precursors studied in these projects is far from complete. The objective is:

(a) Identify and work on chemicals not included in previous projects (PREVAIL);
(b) to obtain better understanding of 'garage chemistry': synthetic pathways, one-pot equipment, micro-reactors etc.
(c) to study the possibilities of preventing their usage for terrorism without harming their normal function or safety properties; and
(d) to design economically feasible methods of practically materialising some of the possibilities identified in stage (c).
(e) to work on recommendations for enhancing the level of security for any precursors to explosives identified as "new" threat chemicals

Proposers should take into account other EU (see above) and national research projects to avoid duplication.

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

Expected impact:
This action should contribute to improve the traceability of chemicals and mitigate their properties that can be used in the preparation of terrorist actions, and therefore contribute to preclude such unwanted use. The action would also provide early information on suspicious use and thus help monitor the use of such chemicals to prevent terrorist events. The action should be complementary to ongoing and past EU actions, as well as currently proposed EU regulatory framework in this matter.

Area 10.1.4 Ordinary crime and forensics

Topic SEC-2013.1.4-1 Smart and protective clothing for law enforcement and first responders – Capability Project

Description of topic:
Law enforcement authorities, private security personnel, disaster relief personnel, and other civilians in hostile situations (e.g. journalists) wear various forms of clothing to protect against deliberate threats against the person and/or various types of hazards.

The objective is to improve current technology and develop a new kind of functionality and effectiveness of protective clothing. An important objective is to provide higher degrees of protection from clothing that can be worn in normal operations. Issues to be included could be: seamless, lightweight, cost-effective, easy to use, wearable for security personnel in real life operations, including innovative concepts for stab/ballistic-resistant wear; sensors; embedded health monitoring of the wearer; communication and positioning linked to command and control. It is also to offer a greater protection over more of the body (arms, legs, feet, hands, head), in particular, protection for very vulnerable points on the body (vulnerable blood vessels, vulnerable nerves, etc).

Proposed projects should build upon knowledge generated in European and national research projects on multifunctional protective clothing. International standards and guidelines for protective clothing should be taken into account. Evaluation methodology, evaluation and validation of the developed technologies are expected.

Proposers can choose to cover only the protective clothing for law enforcement personnel or for first responders.

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

Expected impact:
The projects should offer all intervention personnel a greater protection and increased safety in their daily work, and contribute to standardisation activity and to develop common EU requirements in order to facilitate an EU wide market. It is expected that the outcome of these projects will be developed and validated by the end-user community. A clear potential for exploitation of the results, within the EU and world-wide is expected, given also the interest by the EU to contribute to a growing vibrant and globally competitive European security SME

and industry sector and to generate employment. A significant and demonstrable impact for end-users is also expected.

Topic SEC-2013.1.4-2 Development of a Common European Framework for the application of new technologies in the collection and use of evidence – Coordination and Support Action (Supporting Action)

Description of topic:

Thanks to technological advances in information gathering, Law Enforcement Agencies (LEAs) are able nowadays to obtain evidence, when carrying out criminal investigations, in very effective ways that were impossible a few years ago. However, legislations on criminal procedures in many European countries were enacted before these technologies appeared, thus taking no account of them. As a result of this, three very important problems appear:

(1) The admission in Court of evidence obtained this way is frequently uncertain, giving judges no clear criteria on its admission and assessment, and therefore causing uneven application of the law.

(2) These new technologies can loose their efficiency quickly, as soon as criminal organisations become aware of their existence, obtain technical details about them and adopt countermeasures. The absence of standards and regulations protecting them from having to be publicly exposed during trials, burn them out as soon as they are used. This is particularly valid for criminal transnational organisations, usually having almost unlimited resources.

(3) Globalisation of criminality requires the tight collaboration of the law enforcement and judiciary systems of different countries: evidence obtained in a State has to be shared and accepted in other States, while simultaneously observing fundamental rights and substantial or procedural safeguards. The lack of legislation and standards at the national and international level obviously makes this particularly difficult.

To address these problems a complex set of coordinated developments is required, by different actors, at the legislative, standards, technology and law enforcement levels. A specific framework of standards, guidelines and recommendations is needed. Therefore, the objective of this topic is, from a multidisciplinary point of view, to identify, define, assess and articulate the whole set of actions that should be carried out in a coherent framework, including at least the following aspects:

- A comparative analysis of existing legal provisions which apply in these cases and their impact.
- The identification and definition of those legislative changes that should be promoted both at the European and State level.
- The definition of open standards, assuring not only the international transfer of evidence but also the chain-of-custody requirements and the protection of the means of proof, without forgetting the ethical and privacy aspects.
- Operational and ethical implications for law enforcement agencies (LEAs).
- The identification of those technical developments that should be carried out to sustain all these aspects.

The proposing consortium is expected to incorporate in addition to experts on criminal procedure from a variety of European countries, a significant number of LEAs specialised in information gathering with technological means and at least one R&D technological partner, who should ensure the technical feasibility of the proposed solution.

Funding schemes: Coordination and Support Action (Supporting Action)

Expected impact:
A research agenda covering the issues raised is expected as well as an evaluation of the market size targeted by the technological development. Action in this area should raise sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, international and EU co-operation needs, etc.) and raise the awareness of the EU political stakeholders in order to help them to shape a proper legal environment for such activities at EU level and to demonstrate the added value of common practises and standards.

Area 10.1.5 CBRN protection

Topic SEC-2013.1.5-1 European toolbox, focusing on procedures, practices and guidelines for CBRN forensic aspects – Capability Project

Description of topic:
Forensics research plays an important role in solving crime and maintaining secure societies. Novel methods for CBRN forensics and training would strongly enhance these capabilities.

Proposals should aim to develop and provide a forensic toolbox (either fixed or mobile) focusing on procedures, practices and guidelines for common CBRN forensic measurements and handling instructions on a European level, such that results can be used during legal prosecution to provide solid and court-proof forensic evidence in and after CBRN incidents. This includes practices for sampling, preservation, shipping and storage, analysis, laboratory equipment and recording in the context of criminal events. Guidelines and procedures should include issues like Good Laboratory Practice (GLP), Quality Assurance (QA), Quality Control (QC) and Standard Operating Procedures (SOPs).

Whilst developing procedures, practices and guidelines, projects should give adequate attention to aspects of usability, societal acceptance and economic and legal viability, through appropriate research, experimentation or demonstration in realistic, complex and scalable scenarios and contexts.

Proposed projects should build upon knowledge generated and liaise with on-going FP7 funded and nationally funded projects in the forensic area. Where necessary new technologies should be developed for sampling, analysing evaluating, interpreting and recording forensic evidence with a view to achieve court-proof results.

Common European CBRN forensic procedures are indeed useful to provide guidelines on how to act in CBRN incidents, in particular how to sample, analyse, evaluate, interpret and record forensic evidence and achieve court-proof results.

Testing and validation on the field with relevant end users are expected in order to illustrate the EU added value of such an initiative. It should also include key qualitative and quantitative indicators to measure progress or results achieved during the project compared to the state of the art.

This research relates particularly to the goals outlined in the EU CBRN action plan.

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

Expected impact:
On security of citizens: This project will make available common procedures, practices and guidelines for CBRN forensic aspects. It will therefore provide a solid legal hold concerning CBRN forensic aspects. Potential users of the expected developments will be both public and/or private users.

On industry competitiveness: this project should deliver common procedures, practices and guidelines, as well as where necessary new technologies, leading to common methods for CBRN forensics. Thus industry will have a solid and common basis to develop and deliver appropriate products for forensic analysis. While the market for such technologies is rather specialised and limited, it is expected that economies of scale will be achieved by delivering a European solution, overcoming fragmented national markets and helping to maintain global competitiveness of the European companies, which are predominantly SMEs.

Area 10.1.6 Information gathering

Topic SEC-2013.1.6-1 Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes – Integration Project

Description of topic:
Law enforcement investigations increasingly lead to very large amount (terabytes) of data. The task is to develop new methodology/tools to derive from these various types of data (text, audio, images, video, etc.) evidence that will be acceptable by courts in Europe. The proposed solution should:

- do an automated first treatment of such large set of data in order to limit the human intervention in the analysis to a minimum;
- propose guidance to analysts in order to help them manage the results of the first processing;
- be able to link and merge information with other sources;
- present relevant highlights to the analysts to allow them to refine the process; and
- integrate tools allowing the treatment of scanned calligraphic documents.

In addition, the proposed solution should propose to develop modelling and simulation in order to test operational procedures and techniques and to facilitate the training of analysts and operators.

Demonstration of the developed capabilities and of their integration is required.

The project will have to deal with the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
It is expected to develop new tools, techniques, processes and procedure to support investigators, analysts in their daily work; to start to develop standardisation activities based on common methodologies, tools, procedures in the forensic area; to raise the awareness of Law Enforcement Agencies (LEA); to raise the training and the technical skills of analysts.

Topic SEC-2013.1.6-2 Novel technologies and management solutions for protection of crowds – Integration Project

Description of topic:
The objective is to develop new solutions (methods and tools) for protecting crowds gathering in short notice and temporary events, such as political rallies, sport events, entertainments shows, rave parties, "facebook events", etc, where the assets to protect are mainly the people and their surroundings. The number of such public gatherings, often involving large crowds, is increasing. They can be hard to manage, generate disorder or be attractive for attacks. The protection of these gatherings is a growing concern.

Novel solutions are needed to handle their security. These solutions should allow a fast deployment /tear down process and an easy adjustment to the specificities of the event (size of crowd, physical perimeter, type of potential risks, etc.). Modularity and mobility are key characteristics, and the same equipments should be used in the various types of events as much as possible. The needs for EU standards should be studied, in particular in view of facilitating the potential equipment market.

These solutions also require tools to understand and analyse the patterns of people activities. Especially within the psychological component, more understanding is needed about physiological, cognitive and social perspectives and on the integration between them, on the individual level, and on those of groups and crowds. The methodologies and tools should lead to a more harmonised and structured, but context-based approach. Besides this, they should be evidence based, generally applicable and demonstrated for a diverse range of scenarios, and completely compatible with the latest insights on ethics and privacy by design.

The research effort should focus on the following aspects:
- analysis of the different types of public gatherings, their evolution, the risks associated and the constraints on protection and security measures;
- fast deployment of various sensors (including self-deploying and autonomous sensors) and access control capacities (including cooperative and uncooperative);
- an architecture that allows a fast deployment of the overall security system as well as the tools to monitor, control and command the deployment capacities;
- scalability of the equipment to fit the specific needs of the event;
- plug-and-play and low energy consumption sensors for surveillance;
- mobile Post of Control connected to "outside" authorities' networks;
- a simulation tool to quickly define the configuration for a specific event, evaluate the adequate capacities to be deployed and to train intervention personnel;
- a tool able to extract structured information from an unstructured and multi-domain source as social networks are;
- intervention strategies on how to apply this knowledge in specific security contexts;
- the effects of these intervention strategies on the effectiveness and efficiency of security professionals in different scenarios;
- intervention strategies on how to apply this knowledge in specific security contexts;

- the effects of these intervention strategies on the effectiveness and efficiency of security professionals and people gathered in crowds in different scenarios; and the
- integration of all these solutions into real systems.

The proposed solutions should be as little intrusive as possible. The potential privacy and ethical issues linked to their implementation will have to be addressed, and corresponding recommendations provided for the management of the deployed system. Security forces should be involved in the project. The research should build on previous EU or national projects.

Proposers need to take fully into account the respect of privacy and the democratic rights of individuals as stated in the EU Charter of fundamental rights. The solution proposed should be ethically acceptable. The creation of an ethical advisory board is recommended.

Proposers should take into account other EU and national research projects.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
The outcome of the project should provide a general architecture of a solution for the protection of crowds, a set of technologies suited for this goal, as well as simulation tools to prepare for the protection of specific events. A demonstration of such a solution, which can be easily and quickly implemented to handle the security of temporary events involving large crowds, will be carried out. The project should also prepare standardisation activity in the area with a view to facilitate an EU market for such systems. Emergency management tools will also benefit from the outcomes of the research by incorporating new information sources and assets that can improve incident reaction times and effectiveness.

Topic SEC-2013-1.6-3 Surveillance of wide zones: from detection to alert – Integration Project

Description of topic
The EU suffers from a lack of affordable solutions for large ground areas surveillance such as for instance rail tracks, energy lines, pipelines, highways, etc.

One objective is to integrate ground and/or airborne sensors, to detect, to identify and localise illicit patterns of activity (detection of change or surveillance 24/7) on a wide area.
The aim of this Topic is to go beyond existing research projects and address the systemic and holistic issues (cost sensors, networks and cooperation of sensors, innovative algorithms for data interpretation, correlation and user interface, etc.). Research should also provide a comprehensive analysis on vulnerability, security of the system itself and related system design methodology. A demonstration of the full system is expected.

In addition the research should cover the gathering of information, its qualification and its use for alerting. Costs, integration, efficiency (positive or negative rate of alarm) and maintenance of the system should also be studied.

Solutions are to be developed in compliance with European societal values, including privacy issues and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be taken into account in a comprehensive and thorough manner.

Proposers should take into account other EU and national research projects.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
The common proposed solutions would benefit many European countries, for transnational applications, and would improve the interoperability in terms of data and information exchanges. Research should also contribute to standardisation activities, interoperability and create a level playing field for industry.

Topic SEC-2013-1.6-4 Information Exploitation – Integration Project

Description of topic:
This project aims to facilitate a leap forward in the capabilities to exploit information.

Police and law enforcement agencies (LEAs) often collect, obtain or possess very large quantities of data and information from various sources. These public authorities have a variety of requirements to analyse these large quantities of data and information to produce actionable criminal information and intelligence.

These entities have needed these capabilities for years, but require further improvements and advances. Research should therefore consider what has already been developed, and avoid developing any of the existing technologies and analyses for a second time. A cost benefit analysis should be carried out with regard to the proposed developed capabilities. Proposers should develop and integrate privacy aspects at the design stage of the research.

The tasks are to:

- manage the explosion of data (static or dynamic) in terms of volumes, speed, variety, content;
- develop and make systematic use of anonymisation techniques;
- undertake content analysis to understand semantic and conceptual meaning of information in order to identify relevant information rapidly;
- analyse data and information in order to identify metadata, patterns while improving data fusion techniques etc;
- conduct rapid searches based on meaning and concept;
- analyse the meaning of information in order to detect suspicious information;
- detect, identify, isolate, and generate evidence of terrorism or serious organised crime;
- generate indicators and warnings of imminent acts of terrorism or serious organised crime, including those within cyber space;

and also to:

- present the relevant highlights of this information to the operator/analyst;
- facilitate training of analysts and operators.

The project should deal with the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

The establishment of an independent ethical advisory board is recommended.

Demonstration of acquired capabilities is expected. The developed capabilities need to be validated by an appropriate group of end-users (national or European LEAs, etc.).

Proposers should take into account other EU and national research projects.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
The output from this research topic should include new innovative, efficient and effective capabilities, approaches, tools, techniques, processes and procedures to support police and LEA, to prepare against, prevent and discover serious organised crime, fraud and terrorist acts taking into account the complex IT of today.

The benefits of this research should include a significant improvement in the prevention, detection, investigation and prosecution of serious and organised crime and terrorism, and thereby to more effective and efficient law enforcement. It is also expected that the results of this research will be tested for their societal acceptance.

Activity 10.2 SECURITY OF INFRASTRUCTURES AND UTILITIES

Activities 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.

Area 10.2.1 Design, planning of building and urban areas

Topic SEC-2013.2.1-1 Evidence based and integral security concepts for government asset protection – Capability Project

Description of topic:
Maintaining government continuity and societal stability after a severe incident is a vital challenge for open western societies; both in their homeland and abroad through embassies and delegations. Attacks like the recent Oslo bombings show that the current way of concentrating government buildings in urban areas can be vulnerable. In an urban area, the difficulty is the number of people that are in or nearby a building. This stresses the importance of creating resilience in the functioning of public offices. Security measures on persons, buildings and events are interrelated, but often lack a consolidated approach. This stems from the lack of evidence (study) based security concepts and security management structures. There is a need to do more scientific research to provide a more solid knowledge base for the much needed integral security approach covering both homeland and overseas (embassies, delegations, missions etc), including research into novel technologies that would support such resilience

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

Expected impact:
The challenge is to create the optimal mix of security measures, based on an all risk approach. Proposers should develop security concepts to put these measures in place covering both homeland and overseas (embassies/delegations etc) security issues. This needs to be done in cooperation with multiple other public and private organisations. Undisputed knowledge of the best security concepts is currently missing. The research should result in a knowledge base IT tool that shall provide educational programmes for the management of security and pave the way for a more integral security approach. It should help (public and private) professionals dealing with security to better coordinate building security, with closed protection and event security. Moreover a common European approach of this issue should be taken into account.

Topic SEC-2013.2.1-2 Impact of extreme weather on critical infrastructure – Capability Project

Description of topic:
The frequency of different natural catastrophes caused by extreme weather conditions induced by climate change is expected to increase. Centuries old buildings have suddenly been demolished by floods, earth slides, or hurricanes. Power delivery has failed during heat waves. The functioning of critical infrastructures (electricity generators, telecommunications, public health, transportation, financial services, food and water supply, etc.) are more and more threatened because of the changing weather condition, including drought and heat waves, some of which societies are unprepared for.

The regionally differentiated risks need to be reassessed. A better understanding of factors and the elements to include in risk analysis of societal security should be developed. Moreover, research work under this topic should identify in a systematic way the European and national critical infrastructures that should be re-assessed for extreme weather risks. Technologies to protect against extreme weather should be reviewed and beyond the state of the art improvement should be developed.

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

Expected impact:
The project should bring together climate researchers, meteorologists, first responders, with critical infrastructure owners, operators and planners. A review of European critical infrastructures needs to be carried out - those that are most threatened by various risks are to be identified and classified. Measures to protect these should be suggested so major catastrophes and/or cascading effects could be prevented. Simulations are to be performed and the effectiveness of the measures needs to be quantified.

Specific feature: Projects selected under this topic will be linked through a coordination mechanism that will be defined during the negotiation stage. Coordination with related actions under the Environment Theme[22] will also be established. Costs of this coordination will be covered by project resources.

Area 10.2.2 Energy, transport and communication grids

Topic SEC-2013.2.2-1 A research agenda for security issues on land transport – Coordination and Support Action (Coordinating Action)

Description of topic:
The objective is to develop a research agenda which provides concrete answers to what type of security related projects should be developed in the future. Different transport modes i.e. road, rail, air, maritime (through ports) and inland waterways have become more integrated and have thus created new security risks that need to be carefully managed. Terrorist have taken the transport sector to be an easy target (stations, tunnels, urban transport systems, etc). The task is to analyse the different land transport modes and their interconnections points from the point of view of security and to develop a future research agenda for this sector.

Funding schemes: Coordination and Support Action (Coordinating Action)

Expected impact:
The study outputs are therefore expected to provide a clear state of play of security issues in land transport, including looking into new threats such as cyber attacks. This implies that the interconnection and the integration dimension should also be taken into account. Moreover global guidelines on enhancing the surveillance of the land transport infrastructure in order to ensure the security of citizens and of critical infrastructure against terrorist threats should be assessed.

Topic SEC-2013.2.2-2 Toolbox for pandemics or highly dangerous pathogens in transport hubs – Capability Project

Description of topic:
Natural or deliberate release of pathogens in large transport hubs (railway stations, bus stations, airports, etc.) could affect people travelling across Member States borders and have a major impact across the EU and even other countries. Worldwide travel of people for both

[22] See Work Programme Environment: ENV.2013.6.4-4 Towards stress tests for critical infrastructures against natural hazards – FP7-ENV-2013-two-stage

leisure and business is increasing and as a consequence, probability of uncontrollable spread of infectious disease is also increasing significantly

In this context, the aim of the proposal is to provide at least one of the two following outcomes:
1) Guidelines for first responders and transport operators to prepare and handle pandemics situations in transport hubs. Proposed guidelines should be tested in a variety of large stations across the EU, with the strong collaboration of the end-users and transport authorities. The guidelines should, in particular, focus on coordination capacities for the different security and safety agencies, and also transport operator management teams, to provide unified response based on event-based information sharing. They should take into account local and national particularities and experiences.

These guidelines should be easily understandable and accessible for operators/end users and possibly translated in national languages if required by end-users. They should be widely shared and disseminated among first responders and transport operators. The use of common symbology is encouraged to avoid translation barriers.

2) An integrated toolbox to prepare for and respond to a deliberate release of pathogens in a major transportation hub.

It could include (not exclusively):
- Reference scenarios
- Incorporation of prevention and surveillance tools and technologies
- Rapid detection capacity
- Operational guidelines at the incident site level as well as to the cross border level
- Decontamination tools for the crowd and the facility
- Tracing tools for the potentially exposed, focusing on the multi-national aspect of major transportation hub.
- Epidemiological investigation tools focusing on the cross border dimension and required cooperation.
- Legal and ethical study of the implications of an incident involving multiple nationalities, possibly vessels of foreign countries and the acceptability of the suggested measures.

The proposal should take into account technologies and results of FP7 and national projects in this area, as well as other ongoing EU policy activities in this area (e.g. Health security initiative). Their complementarity and added value should be explained and justified.

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

Expected impact:
Objective 1) Final guidelines (following assessment and testing by end-users) will provide a clear view of the possible threats of pandemics to transport sector in transport hubs and give orientation on how to deal with the pandemic issues. They will contribute to improve the rapidity and safety of rescue operators and save lives (both of potential victims and rescue teams).

Objective 2) The project should create a clear threat analysis to the occurrence of a deliberate release of a pathogen in a major transportation hub in Europe. It will provide an integrated toolbox and will lead to a comprehensive view of the cross border implications of such an incident, accompanied with the tools to – rapidly detect the incident, mitigate its effects on the

site, and respond to the dispersal at the site level and mainly at the multinational level dealing with tracing of the patients, off site decontamination of vessels and sharing of information.

Topic SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks – Capability Project

Description of topic:
A smart grid[23] is an electricity network that can efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power systems with low losses and high levels of quality and security of supply and safety. The future energy distribution network (smart grid) requires such services to be implemented that can monitor in real-time the overall conditions of the grid system and its main components; reduce vulnerabilities and minimise the effects of an attack. The objective is to analyse the smart grid system and then to develop ways to make the system more resilient and less vulnerable to cyber attacks. Methodology and tools should be developed for a high-level security risk assessment in order to minimise the impact of cyber attacks on the smart grid. Moreover, the project should contribute to raising awareness of stakeholders.

Proposers should also take into consideration the use of smart meters as part of the smart grids. The use of smart meters should however be closely analysed regarding its compatibility with EU and national legislation.

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

Expected impact:
Proposers will provide a clear view to policy makers and other stakeholders of the possible threats of cyber attacks on smart grids. Manufacturers and providers should be encouraged to include security measures and procedures in their devices and equipments. Most importantly the proposed research shall assess the vulnerability, propose new security standards/technology, monitoring tools, carry out tests, demonstrate scenarios and propose materials to improve the resilience of the smart grid. Demonstration activities should be envisaged under almost real conditions, using a comprehensive interoperable smart grid/smart metering test bed able to evaluate the performance of the whole system. Cost assessment of the development and implementation of the protections should be included.

Topic SEC-2013.2.2-4 Cost effectiveness of security measures applied to renewable/distributed energy production and distribution – Capability Project

Description of topic:
Energy production and distribution are part of critical energy infrastructure. With the increasing use of renewable energy sources, the number of production points is increasing, so transmission and distribution networks are getting more complex. Currently there are no cost-effective security systems for wide area protection (e.g.: electrical distribution grids, solar farm, wind farm). This makes energy grids vulnerable to attacks. Renewable and distributed energy production should be economically effective for providing supply and ancillary services to help 'operators to operate' their networks, for example, providing voltage control

[23] See the definition from the EU Commission Task Force for Smart Grids at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf

and reactive power support. The objective is to analyse the risks and threats related to this architecture and the development of cost-affordable technologies to protect them.

Funding schemes: Collaborative Project (small or medium-scale focused research project)
Expected impact:
Through an innovative and cost effective approach the research should analyse the added complexity and vulnerability introduced by renewable/distributed energy into "conventional energy grids", to detect the most sensible points and to develop cost-effective solutions to provide early warning of suspicious activities in a distributed energy grid. The system will take into consideration the special characteristic of the renewable energy infrastructures (wide open areas), designing a solution which both respect privacy and is easily deployable. Moreover, the research shall provide a common European approach related to this issue.

Topic SEC-2013.2.2-5 Security of ground based infrastructure and assets operating space systems – Capability Project

Description of topic:
The task is to assess the vulnerabilities of the space control ground stations, in particular those used by earth observation and satellite navigation systems, and secure communication links to satellites which are seen as critical infrastructure and when possible to propose new methods of protection without making strong assumption about the satellite itself.

The research shall focus on the following points:
- Develop risk assessment tools in order to identify specific vulnerabilities of the space control ground stations;
- Develop risk assessment tools in order to identify specific vulnerabilities of the telecommunication links with the satellites and the space control ground stations;
- Develop tools and where necessary new technologies to protect these critical infrastructures (facilities and telecommunications links but excluding the satellite itself) against deliberate acts of terrorism, sabotage and cyber attacks etc; and
- Due to the distributed network architecture of the space control ground stations, carry out contingency analysis that shall provide an innovative and cost effective plan for an automatic restoration and intelligent reconfiguration in case of failure of a part of the space control ground stations network.

These sites can be targets of deliberate acts of (cyber) terrorism, sabotage, criminal activity, malicious behaviour etc. or they can simply be affected by accidents, natural disasters, negligence and so on. Therefore if they are destroyed, damaged or disrupted it can have significant impact on the global space communication and use of space applications. Furthermore it could impact on the overall functioning of the society (security of telecommunications assets, strategically and economically etc).

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

Expected impact:
It is expected that action under this topic shall provide significant improvement in the security and resilience of complex interconnected space control ground station networks. Research shall analyse in an innovative way the vulnerabilities of the different parts of the space control ground station network and provide state of the art tools and innovative solution in order to limit the impact of accidents/attacks etc on these networks.

Area 10.2.3 Surveillance

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

Area 10.2.4 Supply chain

Topic SEC-2013.2.4-1 Phase II demonstration programme on logistics and supply chain security

Description of topic:

The European Union (EU), and nations around the world, depends upon the efficient and secure transit of goods through the global supply chain system (i.e. the network of assets and infrastructures by which goods are moved from the raw materials transportation until they reach an end consumer, as well supporting communications and information sharing infrastructure). This system is a critical infrastructure essential to both the EU's economy and security. Indeed, the same interdependencies that promote economic activity also serve to propagate security risk.

For this reason, the EU needs to maintain or improve supply chain security levels, whilst also expanding transport and logistics networks to enable industry throughout the Union to have effective access to the Single Market and the international markets.

Protecting and securing the supply chain from exploitation, and reducing its vulnerability to disruption, goes in parallel with the promotion of a timely and efficient flow of legitimate commerce. Security processes are to be integrated into supply chain operations whilst ensuring that process efficiency is maintained or even improved. Any solution to be developed should strike a balance between public and business interests, within recognised regulatory constraints.

What is needed is a European approach to a system that operates in an international context and supports the implementation of the various EU security and information management policies and directives, with evolving international regulations and standards, whilst at the same time offering tangible benefits to involved stakeholders (transaction, transport, regulatory and financial stakeholders), thus facilitating its adoption by commercial entities.

The challenge to maintain or improve security levels, while also improving the facilitation of movement of goods, is a difficult one. The likelihoods, scope and economic consequences of illicit trade and organised crime/ terrorism/ disasters related acts, and transport infrastructure failures, cannot be fully anticipated. Efforts are needed to foster a resilient system that would be better prepared for, and can withstand, evolving threats and hazards, and that can rapidly recover and react on disruptions. The efficiency and degree of success of security measures (covering awareness, prevention, protection, detection, response and recovery) are difficult to quantify. Improving security requires an integrated research and development approach, including risk assessment, traceability, secure exchange between nations and across operators, and fast but effective screening. Large scale R&D pilot implementations of integrated approaches are possibly the only route to catalyze the critical mass required to discover the practical problems and to propose solutions that could deliver sizable and sustainable progress in supply chain security across all EU Member States/Associated Countries and on a global scale.

There is a consensus worldwide that the implementation of security policies should be risk management based, cost effective and efficient for supply chain processes. Given the intrinsic complexity and the division of their institutional roles, public security (i.e. police, inspection, law enforcement) authorities find it hard to cover the supply chain holistically. Their efforts need to be harmonized with those of customs and transport authorities. In addition, cooperation between the public and private (business) domain (i.e. shippers, forwarders, terminal operators, transporters, insurance) is essential to develop a coherent security approach. Indeed, it is very much also up to the private sector to develop and implement its own security measures (i.e. to prevent an incident from happening or those aimed at getting an interrupted supply chain back into shape as soon as possible).

In order to maximize the flow of legitimate trade, new mechanisms to minimize the security disruptions and facilitate low risk cargo and appropriate processes to simplify trade compliance should be envisaged and refined incentives proposed to enhance the collaboration of stakeholders. Targeting capabilities are only as good as the data gathered: the customs consider reliable, accurate, complete data for efficient risk analysis as the key enabler for the security of the supply chain.

Customs control for internal security purposes as well as consumer protection, health and safety purposes has been an integral part of customs control work at Member State level. Since the 2005 'Security Amendment' of the CCC in particular, the 'security and safety' dimensions of customs control work have also been incorporated into the customs union policy acquis, and is fully operational since 1 January 2011. The fact that the customs is constantly present at the border and has a longstanding knowledge of the goods moved within the supply chain, places it as one of the primary authority able to detect and prevent illicit and dangerous goods from entering into and leaving the EU.

In practice, customs activity is that of an enforcement authority, which often means implementing the policy priorities of several policy areas at once. Therefore customs co-operation across the EU takes a range of forms throughout the whole EU external border, whether maritime, air or land border. In addition, to respond to multiple types of risks, customs risk management and control must by nature be holistic. This includes the use of state of the art data integration and management systems for risk analysis purposes, the application of a variety of equipment and technology tools for the detection of illicit and dangerous goods, sophisticated laboratory testing for security and safety as well as for fiscal purposes. Furthermore, customs carries out control at the most effective place/moment of the supply chain, which requires efficient communication systems and also the use of modern audit approaches (system-based approach) and post clearance type of controls. Customs thus has to use a variety of co-operation approaches, risk management and control working methods, techniques and equipment.

The Commission coordinates customs risk management related to international trade with third countries, enhances supply chain security and trade facilitation through management of the EU AEO programme, international mutual recognition thereof and the development and use of innovative technology to detect illicit cargo.

Data platform concepts and proprietary systems have so far failed to achieve wide acceptance, remaining restricted to niche markets and to few stakeholders. Indeed, they rely on trusted partners willing to share data (such trust may not be present in the commercial competitive environment, where information related to the supply chain may also represent a key asset for business). The definition and guarantee of the control and the sovereignty of data (who owns

the collected data?) is an important issue to be taken into account. Another issue to be taken into account is the cost vs. benefit for security devices/systems.

In this general context, the scope for capacity building via this demonstration project/programme is identified in the following areas:

Tools & Standards

- Facilitation and expedition of the smooth flow of legitimate trade through the use of multilayered risk management tools and mutual recognition of international trade facilitation programmes that build redundancy in the system, so security breaches can be addressed in subsequent levels. Also aspects of traceability and inviolability are paramount to be addressed.
- Reduction of the costs of security controls, by recognition of the high standards of the controls performed by other authorities,

Prevention & Protection

- Prevention of illicit movement of dangerous and illicit material throughout the supply chain, like trafficking, contraband and fraud, terrorism (including cyber-terrorism or dual use of goods with malevolent intentions) or piracy.
- Protection of critical elements of the supply chain system and the consequent threats to the economic and civil society from attacks (including cyber attacks), theft and disruptions (i.e., unlawful interferences in the supply chain flow), via better understanding and addressing of vulnerabilities for criminal exploitation and to natural events,

Resilience

- Building the resiliency of the supply chain (to either man made or natural events).

Whilst technology plays a critical role in ensuring the security and efficiency of the supply chain, it must be stressed that the appropriate use of technology is only one element in the layers of defence to protect against the range of possible traditional and asymmetric security threats. Technology addresses the potential weaknesses of other implemented layers, therefore it does not replace a credible advance cargo (and people) risk assessment based on sound data. In addition, the importance of the human factor cannot be underestimated. Physical transportation security and cargo monitoring needs to be complemented by good practices, guidelines (e.g. for security awareness and risk management), standards and regulations (e.g. for authentication, certification and data protection), and by properly trained and equipped personnel.

The association with multilateral organisations with responsibilities for possible components of the proposed solutions (such as WCO, ICAO, IMO, ISO or UPU) is considered as an additional asset for the project/programme to attain its goals, with a view to the possible international promotion of mutual recognition of trade partnership programmes and controls, and of security measures.

The proposed activity should not duplicate R&D already undertaken by other FP7 activities. It should rather, where appropriate, critically take account of the outcome of such projects, particularly in terms of integration of systems, data harmonisation and standardisation.

The demonstration priorities between the supply chain disruptions, crime types and terrorism should be based on solid economic and societal impact assessments, such as incidents with the highest total economic impact; worst damages to governments and citizens; worst (physical / financial / reputation) damages to cargo interests and logistics operators; broad facilitation of other (more lucrative) crime types; and (foreseen) growing trends in crime and terrorism.

The proposed programme may consist of parallel coordinated projects (as part of the same grant to ensure an integrated approach). In this case it will have to be firmly structured on the basis of clearly defined objectives and representing different supply chains/freight flows and could be based on economic or activity sectors which are key for boosting Europe out of the crisis because of their economic or social relevance. The project/programme should consider all relevant types of actors (customs, administrations (including public services such as postal supply for packaging distribution), transportation authorities and operators, private sector, etc.) cover different modes of transport (as appropriate), considering the most relevant categories of cargo (ISO, container, semi-trailer, swap bodies) from end-to-end.

A basic element of a successful project/programme will be the active participation, from its initial definition phase, of customs regulatory agencies and law enforcement authorities, together with other agencies nationally and internationally involved in the security of the supply chain. These authorities should be complemented by industrial (e.g. technology and integration providers) and commercial companies, with a focus on consignors, consignees and logistic service providers. The proposal should outline the benefits and incentives expected for all the parties involved. In particular, it should address the requirements and benefits of end-users (shippers) through combining their needs for facilitation and cost and processes efficiency with enhancing supply chain security.

Work is suggested to be undertaken on the basis of scenarios, simulating real operational conditions, following the setting of priorities on the basis of identified threats, risks (including novel) and security gaps, also with a view to assess resiliency (in terms of business processes) and good practices. The field-testing may provide evidence about the strengths and weaknesses in identified individual areas of the supply chain.

In as much as national supply chain security policies will be ineffective unless they are supported by enhanced international cooperation to guarantee their coherence, compatibility and cost effectiveness, proposers for this topic should look for an enhanced international cooperation (as described in Part I of the work programme).

The valuable participation of qualified research performing SMEs shall be considered as a factor of merit of the proposal.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:

The demonstration project/programme is expected to deliver tangible results at its end and to provide an impact analysis for the proposed supply chain measures. In particular, it should demonstrate the potential to increase the overall level of security, by integration of the security requirements without disrupting logistics process flows. Adequate measures shall be demonstrated for securing business (i.e. costs vs. benefits, performance, practicability, and

acceptance) and performance standards, and requirements for such measures provided (to be also acceptable by SMEs).

Solutions are expected to demonstrate the added value of integration of systems and processes to contribute to more secure international supply chains. More specifically they should contribute to:

Tools & standardisation

- propose, towards end-to-end supply chain security, an appropriate mechanism for transparent multi-hazard risk assessment, which identifies not only the specific risks in the chain, but also correlates with the methods applied by public authorities (e.g. the risk method developed for the AEO);
- increase the overall security of the supply chains by fostering harmonisation, standardisation, mutual recognition, responsibilities of stakeholders and interoperability maintaining the efficiency level and the costs of trade, thereby enhancing mechanisms for the secure exchange of security information;

Prevention & Protection

- what will be the possible solutions to new risks and threats required to secure supply chains in 2020? How to protect the EU and its citizens against these new threats.
- identify suspicious cargo (people), as early as possible, through the provision of reliable and sufficient data including “who” is shipping “what” to “whom”, “when” and “by which means”, whilst streamlining the exchange of information with Customs/authorities and facilitating the flow of legitimate trade;

Resilience

- improve supply chain resilience (also to uncontrollable events) using risk management principles, contingency planning and enhanced real-time reaction capabilities;

Cost effectiveness

- deliver collateral benefits, especially higher cost effectiveness for transportation and supply chain systems to stakeholders (incl. SME) as an important factor for ensuring broad acceptance.

Solutions are expected to be tested in terms of practicability for commercial and logistics business, with a coherent ensemble of tests covering multiple modes of transport, actors and multiple categories of cargo, within a multi-layered approach. The potential for standardised application procedures, enhanced information sharing, and security audits, to be conducted jointly by appropriately designated competent agencies, should be evaluated.

For these reasons, the impact of the proposal will be assessed on its potential contribution (where appropriate) for:

- the testing and authoritative validation of technology / process integration (with a view to its future take up), on the basis of appropriate scenarios, including verification and detection capacity, as well as threat assessment and risk management,
- the proof of concept in the provision of timely and accurate data to whom (particularly customs, law enforcement authorities and business partners), and by when, it is needed in the supply chain,

- the proof of concept concerning the return of investment for private stakeholders and for availability of good quality data for public authorities (on global scale), opening novel options of robust security measures,
- the extension and cooperation for the sharing of good practices, opportunities for common certification practices, and contributions to the setting of international standards,
- interagency cooperation and coordination to achieve better integration of customs security procedures with other (border) security controls, in order to enhance security and efficiency at a lower cost for trade and public authorities,
- regulatory bodies to stay in tune with technology,
- the refinement and expansion of resiliency protocols within the WCO, IMO and ICAO, including the support to the development of guidelines, as applicable to the transport modes (air, land, sea) considered,
- driving standardisation in the application of supply chain security measures and supporting the creation of an EU and world-wide market for EU security methodologies and technologies,
- the proof of concept of a resilient supply chain from the business perspective, allowing companies operating in the EU to reduce risks and assessing positive impacts in business models,
- increasing security while maintaining or improving supply chain performance from the business perspective,
- seamless adoption and acceptance of the demonstration items by end-users including: authorities and public services (such as postal supply for packaging distribution), commercial companies, logistic services providers and shippers.

Topic SEC-2013.2.4-2 Non-military protection measures for merchant shipping against piracy – Capability Project or Coordination and Support Action (Coordinating Action)

Description of topic:
Piracy, a phenomenon widely thought to have been successfully eradicated in the 20th century, has as a consequence of failed states, managed to have an unprecedented revival lately. In key trade route choke points like the Gulf of Aden, it is threatening our trade fleets. Addressing the root causes of this phenomenon is a long term process having complex implications. In the mean time, short-term solutions are needed to protect merchant shipping. While dense EU and international military presence in the 'hot-zones' proves to be effective, the costs of such operations are high and naval assets spread thin. Alternative more cost-effective solutions to avoid, thwart or escape pirate assaults are needed. The main goal of this topic is to help protecting EU merchant fleets and maritime supply lines from criminal abduction and harassment. As "classical" approaches like convoys have proven to be ineffective and costly to deter modern pirates, other cost-effective means will have to be investigated. Therefore a thorough analysis of potential non-military counter-measures and approaches is needed based on hitherto best practices and experiences like:

- Comparison of experiences with “active non-lethal defence measures” versus “passive evasion measures”

Two general approaches for civilian ships countering actual piracy threats of becoming seized may be considered. Active non-lethal counter-measures (like water cannons, treated hulls to deny pirates attaching attack ladders or having ships accompanied by professional security guards) are effective but pose risks of escalating towards more violent tactics by pirates.

Passive evasion measures like higher cruising speed and evasive manoeuvre patterns reduce risks for the crew but increase costs and travel time and if they are the only method of defence they leave the vessel helpless in the case of the pirates successfully countering these efforts. Research would contribute to analyse the costs and benefits of both approaches may consider new solutions and potential combinations of both strategies for complementary advantages while estimating the costs and trade-offs emanating from such new solutions.

- Implications, legal pre-requisites and potential societal impact of using civil and/or private security companies to take over certain merchant protection tasks from the military

The use of civil and/or private security companies to protect Europe's fleet is source of heated debates. The issue of private security personnel under arms however remains controversial and hitherto legally opaque. The purpose of research work here is to investigate the possibilities, the legal limits/necessities and the level of societal acceptance for the potential use of such private companies to protect our civil/trade fleets. Conducted research should also determine ethically and socially acceptable technical measures to deal with piracy assaults especially on large ships and vessels without resorting to the use of lethal force.

In considering the wide array of ongoing actions in the field of countering pirate assaults it is essential to avoid the duplication of measures and the creation of isolated solutions. Therefore, an active involvement of the relevant European Commission services and EUNAVFOR is essential. Related research projects and actions on EU and national level like SECTRONIC and VESCOSUR and their respective activities/results should be taken into account as well in a successful proposal. An overview and analysis of ongoing non-EU non-military initiatives to counter pirate assaults should also be considered to accomplish the whole picture of existing counter-measures and trends in this field.

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

Expected impact:
Relevant civil stakeholders / end-users should be provided with an exhaustive practical guide on active and passive contemporary measures to counter pirate threats and their legal, economic and societal implications. Advantages and disadvantages of these measures should be highlighted and realistic improvements proposed. The results should be presented in a well structured and functional way (e.g. in form of a manual) to aid in the usage and further development of counter piracy measures. An automated decision support tool can aid the operator with real time threat assessment and help him determine the best course of action in case of a threat. Such a tool could also provide training and planning capability. Thereby successful projects would provide important support for securing Europe's maritime supply lines and forcing back the resurgent scourge of piracy.

Area 10.2.5 Cyber crime

For this area of the work programme attention is being draw to related activities of the European Defence Agency (EDA). For further details see the website of EDA (www.eda.eu).

Topic SEC-2013.2.5-1 Developing a Cyber crime and cyber terrorism research agenda – Coordination and Support Action (Coordinating Action)

Description of topic:
The objective is to develop a research agenda which provides concrete answers to the following issues: In what categories can we subdivide Cyber crime and cyber terrorism? What are the major research gaps? What are the challenges that must be addressed? What approaches might be desirable? What needs to be in place for test and evaluation? To what extent can we test real solutions, etc.?

Funding schemes: Coordination and Support Action (Coordinating Action)

Expected impact:
The study outputs are expected to provide complementary guidelines on enhancing the surveillance of Cyber crime in order to ensure the security of citizens and of critical infrastructures against cyber threats.

Topic SEC-2013.2.5-2 Understanding the economic impacts of Cyber crime in non-ICT sectors across jurisdictions - Capability Project

Description of topic:
The aim is to measure and analyse the economic impact of Cyber crime on non-ICT sectors (i.e. transport, energy, finance, health etc) and analyse the criminal structures and economies behind such crimes.

Proposers should also create a taxonomy and an inventory on crime committed against non ICT sectors through the use of communication networks.

The research shall foster the understanding and the awareness of the non-ICT sectors and furthermore it should present effective measures for the management of risks related to Cyber crime. Research should develop concrete measures and methods to deter possible criminals and to drastically limit the attractiveness of such crimes.

It goes without saying that the European dimension, jurisdiction implications and interdependency on the involved domains shall be taken into account.

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

Expected impact:
The research shall increase the awareness of policy makers. It should increase the trust and confidence of EU citizens in using cyber applications. It should furthermore help businesses to provide crime-proofed applications.

Topic SEC-2013.2.5-3 Pan European detection and management of incidents/attacks on critical infrastructures in sectors other than the ICT sector (i.e. energy, transport, finance, etc) – Integration Project

Description of topic:
The objective is to improve the detection and management of highly sophisticated security incidents/attacks, including cyber attacks/incidents against critical infrastructures (i.e. transport, energy, finance, and water supply sectors) by enhancing a pan-European and shared situational awareness of vulnerabilities, threats and events. While multi-country/continent wide methods for managing cyber attacks on ICT assets in telecom networks exist today, arrangements for other critical infrastructures are less developed. The methodology and tools to be developed would aim to connect security operation centres at the level of Member States/Associated Countries and operators of such infrastructure, within a collaborative platform which would allow a pro-active protection and fast defence response across multiple domains in heterogeneous networks and systems.

The research shall aim at building the following capabilities: sharing of sensitive technical information collected nationally through secured exchange protocols, providing an adequate early warning system to identify incidents rapidly, coping with rapidly evolving constraints in a scalable and flexible way. The research should pay attention to aspects of usability, societal acceptance and economic and legal viability.

The research shall also include research into solutions and systems for managing, analysing and visualising large data streams or data sets from sensors in order to identify and assess threats. It shall also include research into technical, organisational and regulatory solutions to create a secure environment for the sharing and dissemination of information on threats with relevant public and private parties in order to facilitate preparation and response.

It will investigate how to promote adoption of good practices across sectors. The research shall include a stock taking of existing practices in terms of regulatory or voluntary reporting to competent authorities of security incidents/attacks.

The project should integrate all the capabilities developed or acquired in a coherent shared platform where authorised users could register and exchange meaningful information. A full scale demonstration of the platform is expected.

Many activities have already been undertaken to improve detection mechanisms and to facilitate collaboration in such domain. Related existing activities funded notably under the FP7 Security and ICT themes have to be taken into account. Exiting regulatory framework should be taken into account (directive on critical infrastructure protection 2008/114 EC).

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:

Potential users of the expected developments will be various public and private entities, at national and European level (e.g. EUROPOL) of which active participation (e.g. security operation centres, public authorities and relevant EU agencies) should be sought for.

The action should be an opportunity for networking and exchange between the stakeholders to facilitate the emergence of common European standard.

This platform is seen as an essential step to develop secure collaborative detection and management networks environments for critical infrastructure sectors in Europe.

Topic SEC-2013.2.5-4 Protection systems for utility networks – Capability Project

Description of topic:
The objective is to categorise different types of utility networks (i.e. water, pipeline, gas, etc, that are loosely or not at all connected to telecommunication networks; but excluding telecommunication networks themselves) that can be considered as critical infrastructure.

The task is to develop processes and policies to prevent new threats trends (like for instance Advanced Persistent Threats - APT) targeted against Supervisory Control and Data Acquisition (SCADA) systems. A special attention should be given to the use of new ways of voluntary or involuntary transmissions through personally owned digital/communication devices used in business day to day life.
The research should also propose to include these particular threats in existing risk assessment methodologies.

Moreover global guidelines on enhancing the surveillance of these critical infrastructures should be assessed and also new innovative methodologies and technologies should be developed in order to minimise the cyber risks and threats to these systems.

The research output is therefore expected to provide a clear categorisation of critical infrastructures in terms of threat sensibilities versus the impact on the population

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

Expected impact:
It is expected that the operators will gain a better understanding of risks against their own infrastructures and minimise cyber risks and threats through new and innovative technologies. It is also expected to increase the awareness of policy makers and to pave the way for new legislation if needed. It should also prepare standardisation activity in this area with a view to facilitate an EU market.

Activity 10.3 INTELLIGENT SURVEILLANCE AND BORDER SECURITY

Activities 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.

Area 10.3.1 Sea borders

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

Area 10.3.2 Land borders

Topic SEC-2013.3.2-1 Pre-Operational Validation (POV) on land borders

Description of topic:
The Security Research Theme aims to promote further cooperation between public authorities (end-users) developing new solutions 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 solutions related to 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 into current surveillance infrastructure of the new capabilities provided.

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 for a particular technology in daily practice, is expected to extend the benefits of pre-operational validation beyond technical development. The identification of innovative applications, business models and procurement strategies is also expected to reverberate in the integration of innovative solutions as a fully operational tool. By acting as technologically knowledgeable validator of new R&D, the public demand side can drive innovation.

The validation of innovative solutions in real operational environments requires a notable effort by end-users at all levels, including technical, organisational, operational and budgetary. Keeping in mind the necessity to directly involve public bodies in charge of border surveillance, the Pre-Operational Validation (POV) concept has been chosen as a way to assess the performance levels offered by innovative technologies in a realistic end-user defined scenario, where a trade-off between efficiency, effectiveness and cost can be aligned with actual needs.

Last but not least, the activities carried out under POV make it possible to integrate and validate at the EU level, in an experimental framework, the achievements of previous initiatives that have explored and studied the different dimensions of components and systems, from their pure technological development to the features of their exploitation.

This topic is presented for proposals to enhance the use by the concerned civilian authorities of innovative technology for border surveillance.[24] The specific objective of this topic is to address solutions for the pre-operational validation of "*Common Application of Surveillance Tools at EU level*".

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/Schengen area. Only selected elements of a European approach to Border Surveillance are to be done at European level, in line with the principle of Subsidiarity. A decentralised approach with national authorities is to be followed in implementation so as to:

- allow the highest possible level of integration with current surveillance systems and infrastructure,
- make use of the existing and future communication channels that facilitate the generation of a Europe wide situational picture and a full operational awareness at the external borders.

The EU Sea Border is currently sufficiently covered by ongoing FP7 activities. On the other hand there is a deficit of land border initiatives. POV research activities are proposed to be oriented to the validation of an adaptive and knowledge-aided multi-sensor infrastructure providing an integrated system.

Indeed, the EU/Schengen land border requires continuous day/night detection and assessment capabilities to provide early warning on unauthorised intrusion across the border by smugglers, irregular immigrants, or people involved in any other illegal activity. At official border crossing points (BCP) there is a continuous prevention and protection against these threats that may affect the security of the European Union. However, actual irregular border crossings are being increasingly performed on foot or with the help of light vehicles outside the BCPs, taking advantage of the terrain and of poor visibility to avoid detection. In remote areas of land borders, where it is relatively easy to irregularly trespass the frontier undetected, the cost of providing and maintaining effective physical barriers is excessive.

Technology has been a trustable ally, but current capability demand requires progress beyond the current state of the art. Tools and systems need to be aligned with current threats, overcoming existing limitations and provide cost-effective solutions in line with the end-users' needs. The evaluation of cost efficient platform/sensor combinations and of systems matching data exploitation is a research priority for Border Guard communities. A POV on land border surveillance should, hence, investigate and evaluate such technologies in live tests carried out under operational conditions defined by border surveillance authorities.

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 be explored. Capabilities intended to provide "early warning" or "detect" observations from EU/Schengen neighbouring countries should be developed in agreement with neighbouring countries.

The topic is to be implemented via the CP-CSA funding instrument, which involves a combination of the collaborative project and coordination and support action funding

[24] The Commission indicated such objective in its communication "EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM (2010) 673 final)).

schemes. It enables therefore the financing, under the same grant agreement, of research, coordination and support activities.

Its aim is both to 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 to 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.

The nature and the objectives of this indirect action are such that it should ideally involve at least three independent public authorities in charge of border surveillance (at local, regional, national or supra-national levels), each established in a different EU Member State or Associated Country. Other stakeholders may participate in addition, if their participation is well justified and adds value to the action, for example (but not limited to) if:

a. they represent an authority or a regulatory body with responsibility in some area affected by the use of a particular technology,
b. their support is required in order to facilitate the technical, administrative, financial or managerial procedures for which national authorities are limited by their respective national regulation.

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 tools for the surveillance of land borders at EU level via the competitive testing and assessment of potential solutions. Tools to be tested may include a variety of platform types deploying sensors for surveillance purposes.

The information acquired by each platform type should be correlated with other available intelligence sources (i.e. airborne or 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:

- the demonstration that there are existing innovative solutions which provide the required additional capabilities;
- the identification of technological solutions for the achievement of a set of user-defined operational objectives;

- the technical feasibility of 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;
- 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;
- the identification of the maturity level showed by 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 evaluation of the experimentation results promoting their widening to future solutions.

As part of the project activities, the industry shall be called to provide solutions to be tested and validated according to the concept developed by the consortium participants. In order to guarantee an independent and reliable validation process of the proposed solutions, a mechanism has to be enabled that supports the activity of the different actors throughout a series of steps.

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 organisations (if appropriate).

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 Needs Analysis Document and 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 of the tender. 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 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.

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).

For implementing this CP-CSA, different constellations for joint validation[25] are allowed, such as for example common validation entity[26], lead authority[27] and piggy-backing[28] 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*"[29]) (CP phase 2) and

[25] "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.

[26] 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. This entity shall be integrated among the project beneficiaries in equivalent conditions in terms of rights and obligations, and support the decision process, facilitating the development of a validation strategy and the arrangements for launching a competitive call for the demonstration of surveillance capabilities.

[27] 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.

[28] 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 make use of the resulting contract a later date (normally during the timeframe of the original contract).

- 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).

It is clear from the above that, in addition to the EU financial support to phase 2, participants shall contribute directly to the research and technological development activities involved in the testing of new solutions. This contribution of the participants to phase 2 can be in kind (e.g. personnel, premises, systems and services).

Expected impact:
This CSA-CP is expected to significantly contribute to the implementation of an EU 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; and
– reduce the number of irregular migrants across the external EU borders.

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.

Through the execution of the project, the adaptation of existing technologies and the research and development of new technologies, participants are expected to verify and optimise their technological choices. Technology providers will increase their understanding of modern operational requirements thus increasing their competitiveness. The project has the potential to create important market opportunities for European industry and establish a clear leadership in this area.

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[30] are fully respected throughout the POV process:

[29] 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

[30] 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.

- 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**[31] **services contract**[32].
- More than 75% of the EU contribution is expected to fund Phase 2 (Preparatory Work and Execution Phase).
- **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.
- **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[33].
- In respect of the Treaty principles the public purchasers shall ensure **EU wide publication** for the POV call for tender[34] 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.
- 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), and the institutions of the European Union, 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

[31] 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.

[32] 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.

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

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

allocation of IPRs, shall be published upfront in the POV call for tender documents. 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[35] 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 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, if appropriate, the format of the intermediate evaluations after the solution design and prototype development stages that progressively select organisations with the best competing solutions.

Topic SEC-2013.3.2-2 Sensor technology for under foliage detection – Integration Project

Description of topic:
Several regions at the EU/Schengen Area land borders have forests. The aim of the topic is to detect, locate, track and recognise persons and vehicles entering EU/Schengen territory irregularly in a forested region.
Surveillance in land borders implies observation over wide distances and harsh unstructured environments. This makes it very difficult for sensors (i.e.) radars to detect hidden objects (both mobile and static). The project should develop a system improving capabilities in operational use for situation awareness and identification of objects and groups of persons of interest (e.g. detection of abnormal behaviour, ability to interoperate with law enforcement bodies in case of incident).

Five complementary technology solutions are proposed for possible inclusion (not necessarily all five) into an integrated system, to be possibly implemented on airborne platforms and/or on ground based towers, so that each technology would be used for what it is best suited, taking advantage of complementarity of the elements:

a) Low frequency radars (UHF-VHF, from 80 MHz up to 400 MHz)**:** They allow rapid scanning of large areas in all weather and lighting conditions, but the challenge is to distinguish the signal of persons and vehicles from the clutter due to variable vegetation and ground reflections and, even more, to detect and recognise targets when they are hidden beneath the vegetation. The technological challenges include better knowledge of natural background clutter and its dependence on environmental conditions; synthetic aperture radar techniques to improve spatial resolution to reduce clutter, polarimetric analysis to better distinguish man-made objects from natural background and a cognitive capability allowing

[35] 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.

dynamic optimization of sensor performance and adaptability to the environment. The analysis of the penetration of vegetation in different conditions as a function of frequency should be done as well, in order to design the best waveforms and systems to be used for foliage penetration. Specific development of wide band transceivers and receptors for increasing the precision of localization and tracking will also be needed; and this may require algorithms for detection, location, tracking, and identification.

b) Hyperspectral imagers: This imaging technique provides wide area surveillance with high resolution and improved capability to detect and identify targets and their traces in complex background through the detailed analysis of target reflection properties. Technical challenges include development of both hardware and software data processing for automatic target detection. If unmanned aerial systems were to be considered, data reduction techniques would need to be developed to enable both fast information and extraction from large hyperspectral data stream and effective transmission to a ground station.

c) Active or passive imaging systems: Laser pulse illumination can be used in all lighting conditions, combined with range-gating technology in order to see through vegetation, camouflage and windows. Active imaging can be applied to detection of persons and vehicles, but because of high resolution, the technique is particularly suited for eliminating false alarms of other sensors and for giving information of the target type (person, type of vehicle etc.). Broadband lasers allow detailed analysis of the reflection properties of a target and improve recognition capability. In this case technological challenges include further development of lasers and sensors, signal processing and new active imaging concepts like synthetic aperture Lidar, multi-aperture systems, photon counting imaging, holographic imaging and vibrometry for target identification.

d) Unattended Ground Sensors: The Unattended Ground Sensors provides a unified and distributed wireless and self-powered sensing network that can be adapted to any environment. The system can use different sensing technologies as seismic, magnetic, volumetric and video, in order to detect intruders in different scenarios, as roads, forest, rivers crossing... The technological challenge is the combination of processing technologies at sensor level to provide local target classification, and at system level to get alarm verification and tracking of the intruders. The communication of the sensors will be reduced to VHF to provide long range communications in forest environments.

e) **High-resolution low-cost time-of-flight 3D camera:** The ladars or lidar cameras are used for measuring absolute distance by the time-of-flight technique (ToF). It is based on calculating the travel time of a light pulse to obtain the direct measures of distance. This technique offers some outstanding qualities such as the ability to perform non-contact measurements of fast optically visible objects at distances from few centimeters to tens of kilometers. The precision of the measurement is around few centimeters. Some of the most important parameters are the precision, measurement time, range and spatial resolution. A substantial advantage over similar techniques such as stereovision regards on the result of the measurement process is directly the distance value, thus saving the need to run complex algorithms for 3D reconstruction. Also, the devices can work in noisy environments such as low light scenes, rainy or dense vegetation spaces generating three dimensional images from the measurement of many points forming dense point clouds with spatial resolution in the order of 2Mpx.

The integrated system implies the fusion of data generated by the different (distributed) sensors, thus an appropriate telecommunication element should be put in place for the management of this data exchange.

The solution should be capable of detecting man made activities with abnormal characteristics (as appropriate), thus the system should be defined in close collaboration with end users (border guards), on the basis of a clear analysis and understanding of their requirements (e.g. performances and affordability), with a view to allow them to plan resources more efficiently (e.g. by using an expert resource management system).

The inclusion of cognitive capabilities is expected to be of help for the improvement of performances (e.g. for automatic classification of the intrusions, the implementation of a unified tracking of the intruder, automatic image verification, reduction of the false alarm ratio).
Following a proper analysis of the technologies to be separately developed for system implementation, the ultimate objective of the project would be to assess performances at the system level in terms of capabilities.

Because much experience has been gained by the defence sector in this area, close cooperation should be sought in order to avoid any duplication of funding.

Legal, ethical and societal implications have to be taken into account appropriately.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:

Impact would be benchmarked in terms of the expected improvement of border surveillance and effective management of incidents. The system should thus be tested and validated in terms of capabilities to:

- control effectively the land border, also where covered by a vegetation layer, enabling better situation awareness. The system should make it possible to more effectively detect and support reaction to (irregular) cross border activities, through the tracking of the intruder and the implementation of early warning strategies (with low rate of false alarm);
- plan more efficiently the use of law enforcing manpower to intercept people irregularly crossing the border.

End-users are expected to validate via real life demonstrations the fitness for purpose of the system, in terms of practicability and cost effectiveness.

The impact of the proposal is also to be measured in terms of potential for marketing opportunities for the EU industry, thus the proposal should present a credible and realistic analysis of such targeted market (worldwide).

Topic SEC-2013.3.2-3 Mobile equipment at the land border crossing points – Capability Project

Description of topic:
A major challenge for border authorities is the need to promote both security and mobility. Travellers require fast and convenient border crossings, whereas the authorities need to secure the EU/Schengen area from border security threats.

Currently, border security efforts focus mainly on airports, where automated border checks (ABC) are cost-efficient. At land border crossing points ABC's are, however, more problematic as they require large infrastructure investments if passengers need to park their cars, and enter the building where the ABC gate is installed. Increasing passenger flows would then require investments on new technologies, buildings etc.

Projects should aim at delivering border authorities more efficient technological equipment that provides higher security level of passenger identity control inside vehicles including in trains, at land border crossing points. What is in particular needed is mobile equipment together with fast and reliable wireless connection that can be used in checking passengers inside vehicles for biometric identification (for VIS and other large scale systems).

Legal, ethical or social implications have to be taken into account appropriately.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

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

Expected impact:
Visa freedom between the Schengen area and neighbouring countries (e.g. Russia) has been discussed for several years. Because visa freedom will increase the flow of people across the EU land border, fast processing is required for passengers within vehicles. Mobile equipment is expected to enhance the security and efficiency of land border crossing-points through the application of biometric technology for identity checks, enabling modern risk analysis of the passenger flows, and guaranteeing the efficient management of the increasing passenger flows. Legal, ethical and societal implications shall be appropriately taken into account.

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-2013.3.4-1 Border checkpoints - hidden human detection – Capability Project

Description of topic:
Technology for the easy, fast and effective detection of humans hidden in a variety of vehicles (cars, trucks, containers, buses, trains etc.) is still not available to border guard services. CO_2, heartbeat and x-ray detectors are all of limited effectiveness. It is highly important to continue to seek new and improved technologies that achieve close to 100% success rates while providing safety, speed and value for money.

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 or potentially problematic from a health and safety perspective, unreliable, or difficult to deploy in all border control scenarios.

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; and
- 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).

As in this area an R&D FP7 cooperative project based on detection of human perspirations is already planned, alternative approaches should be envisaged.

The project should include at least the active participation of one authority officially in charge of border control at the national level.

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

Expected impact:
Today it is difficult to determine how many irregular 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 irregular immigrant is an essential requirement for the juridical treatment of the case.

Impact will be assessed against the fitness for purpose of the developed technologies. Validation should thus be at the heart of the project and should be foreseen in the proposal taking fully into account the responsibilities of the national border control authorities (and the Frontex agency). Border authorities shall be closely involved in the project and the validation strategy should be put in place at the start of the project under their supervision. 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 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. Legal, ethical or societal implications shall be appropriately taken into account.

Topic SEC-2013.3.4-2 Extended border security - passport breeder document security – Coordination and Support Action (Supporting Action)

Description of topic:
A recent study by Frontex on the Operational and Technical security of E-passports[36] identified that the reliability of the e-passport issuance process is vital for EU/Schengen border control. Indeed, since every Member State has in essence the role of a "back-door" into its Schengen neighbours, it is important to ensure that each external border maintains a minimum equivalent level of security and that variations in the e-Passport issuance process are minimised.

If legitimate documents are being issued on the basis of unreliable ones, then border control cannot address this problem. The Frontex report therefore recommended that "structural information exchange between the issuance community and the border control community on e-passport security matters" and that "training (and possibly tool provisioning) for the verification of breeder documents by issuance officers" be provided.

The proposal should investigate:
- the current state of passport breeder document requirements and issuing practice in Member States/Associated Countries;
- identify key common security gaps;
- recommend possible solutions; and
- include feasible and cost-effective training and communication methods.

Funding schemes: Coordination and Support Action (Supporting Action)

Expected impact:
The impact of the project will be assessed in terms of:
- its potential to contribute (credibly and substantially) to the improvement of the reliability of the process of e-passport issuance, redressing security gaps, and its harmonization at the EU/Schengen level;
- the value of its outputs for intensified training of both passport issuance officers, on how to detect falsified breeder documents (such as birth certificates), and of border guards, on the specifics of e-Passports inspection.

Topic SEC-2013.3.4-3 Security checks versus risk at borders – Capability Project

Description of topic:
Current EU and national policy in the vast majority of EU/Schengen Member States prescribes 100%, or close to it, checks on passengers. A great deal of resources (human and financial) is spent on such activity both by the public and private sector. Technological policy approaches have been taken for improving the efficiency of such checks, even to the extent of prescribing which system and equipment should be used by border crossing points (BCPs) –

[36] http://www.frontex.europa.eu/gfx/frontex/files/frontex_study_on_operational_and_technical_security_of_electronic_pasports_public.pdf

irrespective of the threat level or numbers faced but always on the basis that 100% checks give the greatest benefit in security terms in relation to their cost in resource and speed of passage terms. However, there is little questioning of the fundamental correctness of this approach and very little empirical work that would allow policymakers to decide if a more targeted approach would give similar or better security results.
In this topic researchers are expected to:

- "red team" security measures in a number of BCPs of the 3 types across Europe (air, land and sea) facing different numbers of passengers and levels of threat,
- assess the global impact of the different schemes of security checks, including the costs at the user's level,
- assess whether 100% checks are effectively the best way to guarantee security, based on different experimental set ups of security measures,
- assess vulnerability in human, organizational and technical resources comprising the security system,
- suggest an approach for security checks based on threat levels and a dynamic evaluation of risks at individual level, instead of the current scheme,
- propose a (or various) solution(s), based on existing or under development technologies, to implement this approach,
- evaluate the potential areas where additional research should be carried for such an implementation,
- pay a special attention to guarantying the protection of fundamental rights and especially of personal data protection in the proposed solution(s).

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

Expected impact:
Available operational research, for example in airport security, suggests that no system can be completely secure, that benefits drop off rapidly after a certain level of cost and that random checks may well be as effective, or sometimes more so than 100% checks. Moreover, systems and equipment used to create security levels are public and well-known to all potential wrongdoers, thus counteracting one of the most important elements of an effective security measure (the fact that what it is and how it works are unknown to the potential attackers). Authorities also make the point that the best guarantee of security is the overall individual risk-based assessment, and not only the mere carriage of dangerous or prohibited items.
The research is expected to provide an analysis of security levels in 3 types of BCP (air, land and sea) and to propose a detailed approach of border checks based on individual risk evaluation. A credible strategy should be presented for the appropriate communication of the results for the future decision making process.

Area 10.3.5 Intelligent border surveillance

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

Activity 10.4 RESTORING SECURITY AND SAFETY IN CASE OF CRISIS

Activities 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.).

Area 10.4.1 Preparedness, prevention, mitigation and planning

Topic SEC-2013.4.1-1 Phase II demonstration programme on aftermath crisis management

Description of topic:
It is largely recognised that emergency and crisis situations[37] will become more complex, uncertain and unpredictable. Vulnerability of the societies in Europe is inevitably increasing. Whenever and wherever they happen, crisis situations usually deserve a scalable (regional, national, European, International) and multi-facetted approach as they tend to provoke severe and unexpected human suffering, physical, psychological, societal, environmental, economical and political effects that might also easily cross the borders inside as well as outside the EU.

This FP7 Security Research demonstration (the "*demo"*) should develop comprehensive solutions and approaches (e.g. a "system of systems" or a " large comprehensive toolbox") that will contribute to enhance the resilience of the EU societies against future crises, by providing EU-tailored preparedness and response solutions able to allow enhanced performance and interoperability between relevant actors in all its dimensions. It could for example provide a test-bed to promote assessment and acceptance of these solutions and approaches. The aim is not to create a fully new system replacing existing ones; but rather to integrate it into existing systems and projects at local, regional, national and EU level, with a scalable approach to adjust to large scale disasters and evolving situations.

The project should also develop guidelines and tools for the creation of disaster databases and the compilation of reliable, interoperable disaster occurrence and impact data within the European Union.

Since lack of reliable and real time information is one of the main problems in disaster management, current monitoring networks could be coupled with ad hoc technologies (ground

[37] As for example fires, floods, earthquakes, pandemics, weather casualties or environmental contaminations

based , airborne and satellite based) in order to provide a quick damage assessment, which is the starting point for any kind of decision and intervention.

The implementation of this crisis demonstration programme is clearly expected to link policy, research, industry and end-users in order to make it realistic, reliable and useful at the end. It should bridge the current gaps and allow testing and (pre-operational) validation of research solutions that at a later stage could be applied directly for disaster management. The demo should increase our capacity to anticipate and prepare for disasters, inter alia through better monitoring and planning, including an improved use of existing assets and logistics. It should also increase our capacity to respond to disasters.

Coordination is crucial during large scale disasters due to the involvement of a large number of actors and the uncertainty and lack of information that characterise a major crisis. In order to prepare solutions for an improved coordination, the demo should identify and take into account comprehensive and representative scenarios that will trigger as many aspects of the different crisis situations as possible, involving the tactical, operational and strategic level.

The population is always a key actor in crises and disasters, both as the affected and as the very first source of response, both independently and as volunteers in support of professional response organisations. Enhancing the disaster resilience of EU societies means first and foremost preparing the population, thus a strong citizen focus should be an important driver of the demo. In this sense, social networks and their particularities in terms of communications could be taken into account, in particular in the way they can be used for crisis management and post-crisis activities.

Cost-efficiency should be introduced in all aspects of the crisis management activities. As such the demo should include it as a key factor (best use of available resources). In particular, the costs of coordination activities and logistics should be addressed with special care, reinforcing mutual confidence with a rationalisation of end-users' resources.

The demo should present a "next generation" approach to the problems targeted and solutions offered, demonstrating a clear innovative approach, going beyond activities already conducted within the EU.

Link to EU policies
The demo should correspond to EU policy priorities in the area of crisis and disaster management[38], where serious, unexpected and often dangerous situations require immediate action; situations that may affect the lives, infrastructures, the environment or the basic values of EU society.

The demo should in particular contribute to the general orientations[39] for future EU Civil Protection (EUCP) which have been set out in the Commission 2010 Communication *'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance*' and the recent EC legislative proposal for a revised EU Civil Protection mechanism. As addressed therein, there is a need for enhanced prevention and preparedness since this can reduce the potential impact of many disasters.

[38] Including for instance the Floods Directive(2007/60/EC).

[39] Such measures include for example the development of national risk management plans, the development of contingency planning for EUCP operations and the creation of a voluntary pool of national assets.

There is a need for stronger links between all phases of the disaster management cycle and the demo should strengthen these links.

Contribution of ongoing research and lessons learned from other fields and past incidents
A large set of projects[40] related to crisis and disaster management have been completed or launched in recent years within the EU. In addition to this, national-level experiences have also been built and evaluated in this field, providing a wide range of findings which should be taken into account in the demonstration. The demo should therefore build on existing tools and results of completed and ongoing projects, and combining them with legacy systems and tools. The demo should provide a strong contribution to existing structures and financial instruments (EU and national levels).

Knowledge and experience from other fields such as health, environment, transport etc. could be useful and could be brought into the demo if relevant.

Lessons learned from past incidents, preparedness activities and simulations should also pave the way for future actions since lessons learnt are key in improving the system
Integration, testing, validation, field demonstrations
Integration of promising approaches and solutions into existing systems and mechanisms, as well as interoperability between existing technology and its users is essential and should be considered in the demo.

Proposed solutions and technologies, in order to be applicable, have to be accepted and validated by the end-users and finally incorporated into their Standard Operating Procedures. The demo project therefore has to address the way the end-users are processing data and utilising technology in crisis situations.

The demo should only consider mature and near mature approaches that can be brought to operation within the time frame of the project. To date there has been limited (pre-operational) system validation in FP7 crisis management related projects. The demo should therefore put emphasis on testing, validation and iterative improvement of research solutions (including pre-operational validation).

The demo could provide a test bed for testing and evaluating tools, operational concepts and approaches with an active participation of operational end-users. Such a test-bed could would include (methods for evaluation and performance assessment, experiment support tools, and if justified, modelling and simulation in support of testing and evaluation).

These end-users and their respective authorities are those in the best position to define and assess the performance of the tools and solutions developed. These should be experimented in a pre-operational configuration, to be defined by representative stakeholders in different Member States and/or FP7 Associated Countries.

Involvement of en- users and stakeholders
Involvement of crisis and disaster end-users and stakeholders in FP7 and in a demo is challenging but it can substantially influence research outcomes through:

- transfer of practical know-how from experts to scientists;
- conducting of (testing) exercises, training and practical support; and

[40] Mainly FP7 Security Research but not exclusively

- ensuring the acceptance and usability of the suggested solutions, through extensive processes of consultation with those who are to use / be assisted by the suggested tools.

End-users and other stakeholders should bring their expertise, needs and past experiences into the demo, at all levels, including their already existing demo infrastructure and tools.

The involvement of end-users and stakeholders is therefore expected during all phases of the demo:

- during the definition and preparation of the proposal, with practical questions;
- during the design of the actual work, with practical questions;
- during the R&D with experts feedbacks to the researchers and developers; and
- during the end-phase with testing, validation exercises, user feedback.

End-users and stakeholders should be representative of all levels of crisis and emergency management actors, including local, regional, national and international agencies, including public and private entities.

EU added value and the EU dimensions of crisis management
In this demo the focus should be on the internal EU cross border dimension, aiming at meeting the EU internal challenges for Civil Protection and crisis management (interoperability, host nation support, SOPs, organisational structures etc.). There might, however, also be a need to address external crises which directly affect the EU internal security (e.g. pandemics, energy supply, and volcanic eruptions) or which can bring a clear EU added value to the demo (for example like strengthening the EU's visibility in global crisis management). Working on the internal and external dimension is not mutually exclusive, but they may indeed require a distinct approach.

Scenarios and locations for crisis demonstrations activities:
In order to demonstrate their value and potential for future disaster management, the solutions and results will be assessed, tested and validated in joint regional, national and large scale, cross border scenarios under realistic and real time conditions according to a list of selected predefined representative crisis scenarios (a minimum of 3 is expected). These "demonstration" operations should be organised in locations offering a clear cross border dimension and/or EU added value. To allow for optimal cost-effectiveness, the use of modelling and simulation for testing and evaluation could be used to complement live demonstrations, but only if justified.

The definition, preparation and coordination of, as well as lessons learnt from these activities should closely involve local and/or national and/or EU crisis and disaster end users and authorities.

Measurements and indicators of achievement
As an essential part of the demonstration activity, clear, measurable, qualitative and quantitative indicators (and any other reliable evidence) should be presented, such as:

- EU added value;
- usefulness and achievements (including potential for future applications and operations);
- scalability and modularity;
- reliability;

- innovation; and
- affordability and cost-effectiveness (best value for money).

These indicators will be used to demonstrate the level of achievements and success reached in the demo, as well as the potential for future applications and operations

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
It is impossible to foresee all potential disasters and their effects. Therefore, the demo is expected to provide solutions (either generic tools or a coordinated portfolio of tools) that can be used on a daily basis by end-users, but that are also scalable in a crisis and adaptable to different crisis situations as well as changing conditions during the disaster. The demo will provide an integrated framework bringing together the abilities of industry, research institutions, operational end-users and the citizens, to jointly progress in the critical areas of crisis management and to create acceptance for new solutions and approaches. It will therefore help crisis management systems and cross border concepts to adapt to new and changing threats and to the use of new tools.

On preparedness, the demo will integrate the development of methodologies and demonstrations for integrated situational awareness and risk assessment capabilities, notably with a view to reinforcing preparedness for multi-sectorial crises.

The value and potential of solutions provided (usefulness, scalability, modularity, reliability, affordability) for future deployment will be assessed and demonstrated in realistic conditions through clear, measurable indicators. Through this, success and EU added value achieved in the demo project will be described and measured on the basis of a qualitative and quantitative assessment.

Topic SEC-2013.4.1-2 Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and other unfortunate consequences – Capability Project

Description of topic:
Due to strong interdependencies between different sectors in society and between different countries, there is a need to better understand the cascading effect and cross-border effects in crisis situations. This would improve future response and preparedness and contribute to lower damages and other unfortunate consequences. Since this is rarely addressed in current regional/national research activities, that kind of research with a high EU added value would improve the planning for EU Civil Protection and crisis management operations.

The cascading effect in crisis may indeed cause major impacts and damages if the society is not well prepared and not equipped for quick response to such situations. The nature of a crisis (interaction between the physical phenomena and the human activities) often requires prediction tools providing multi sectorial foresight of possible consequences of incidents combined with measures taken by public authorities and first responders including the communication to the public.

In order to be better prepared for and more efficiently take decisions before and during the incident there is a need to develop foresight tools and decision support tools.

This project should first look into different representative crisis scenarios and identify the different originators or large scale disasters and their dependencies with other crisis originators and aggravating factors, thus identifying the possibility for a "cascading effect". The result of this should be a model and/or methodology to identify dependencies and the events leading one to the other.

The project should also identify the human activities in the crisis – their impact on the event, and the impact of the event on the human behaviour. The project should have a wide approach looking into the general public, the media, the first responders and their commanders and the decision makers at different levels. This model has to specifically identify the key points in the incident evolution where decisions are needed, and identify the type of decisions needed, including preventive decisions.

These key decision points should be incorporated into the incident evolution tool. The tool should enable the simulation of different scenarios (different physical phenomena, different decisions at different point in time) and their effect on the end results, in order to provide decision makers, incident commanders with the capacity to test their emergency and contingency planning. The tool has to be user friendly to the degree that it will enable the use during an actual crisis to improve the decision taking. It should identify critical decision points and bottle necks. It has to be designed to support cross border operations and
The tool has to be developed in close cooperation with end-users – first responders, emergency managers, decision makers, while taking into account a wide European perspective. An extensive training module for the end-users could also be considered.

The proposal should take in account technologies and results of FP7 and national projects in this area.

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

Expected impact:
The project will produce models of dependencies and effects in crisis situations (of both physical and human components) causing a cascading effect. It will also provide a methodology to create this model for future threats, and tools to foresee the evolution of an incident, based on the physical properties, critical infrastructures properties and risks, human behaviour, the decisions taken and their timing. These tool(s) will be available on real time basis as well as for planning and training purposes, in particular in cross border crisis situations.

Topic SEC-2013.4.1-3 Development of simulation models and tools for optimising the pre-deployment and deployment of resources and the supply chain in external emergency situations – Capability Project

Description of topic:
The objective is to develop simulation models and tools for different crisis situations, which aim at improving planning and preparedness of the various resources and capacities, state material reserves included with supply chain needs in the rapid reaction in external (outside the EU territories) emergency situations. This should apply to both the pre-deployment and deployment of resources and the supply chain.

The proposal should take into account technologies and results of FP7 and national projects in this area. Testing, validation and cross border demonstrations in the field with relevant end

users are expected in order to illustrate the EU added value of such an initiative. It should also include key qualitative and quantitative indicators to measure progress or results achieved during the project compared to the state of the art.

Proposers for this topic should take into consideration the current EU external policy in the area of crisis management.

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

Expected impact:
This project should contribute to improve EU external emergency crisis operations. It will develop a base line for external interoperability of logistics over regions and countries outside the EU.

The following outputs are expected: basic definitions for equipment descriptions and equipment functionality, standard operating procedures, an identified legal framework for the logistics response and technical tools for planning the amount of resources required, their pre-deployment, mobilisation during a crisis, tracking on real time and lessons learned.

Topic SEC-2013.4.1-4 Development of decision support tools for improving preparedness and response of Health Services involved in emergency situations – Capability Project

Description of topic:
Healthcare systems have an essential role to play in the response to emergency situations that in many cases have a negative impact on human's health – varying from direct injuries, diseases, long-term effects of radiation, handicap, to effects on the mental health of the affected population, and the health effects of sudden poverty.

Given the importance of health services in emergency large-scale and/or crisis and disaster situations, the consequences of them being unprepared could be particularly dramatic in terms of casualties, panic etc. Therefore, the development of tools to improve their preparedness and response is of utmost importance.

Although their role in the response is clear, in some cases healthcare services are not perceived as part of the "security" arena, thus tools and procedures for preparedness and response are lacking.

This project should target the preparedness and response phases of the emergency situation by creating:

1. Common grounds for interoperability of medical services in a disaster (at a local, regional and cross border response), by creating a common taxonomy, operational definitions for equipment – descriptions, performance requirement, a suggested minimum training requirement per performance.
2. A threat analysis with relevant reference scenarios.
3. A methodology for preparedness – prioritising the scenarios, creating the required standard operating procedure, identifying the necessary coordination with other stakeholders, identifying the required resources, the necessary training.
4. A methodology for validating each component and the preparedness as a whole. The project should demonstrate this whole cycle with a real health care system on at least two different scenarios.

5. The intelligence and analysis of gathering tools, with the relevant modules to alert the occurrence of an unusual biological event (weak signal detection), predict the evolution of the scenario, create the operational picture and share the information with all the relevant stakeholders.
6. The logistic models for assessing the needed stockpiles of necessary equipment, medications, vaccinations and personal protective equipment, their positioning and restocking (to avoid expiration).
7. The tools used for the creation of surge capacity in the event of a major health crisis. This topic should include the use of volunteers and of cross border assistance (including the legal implications).
8. The coordination mechanisms within the healthcare sector and with other security agencies, nationally, cross border and with international organisations.
9. An analysis of the measures planned to deal with a major health incident, their social acceptance, legal and ethical implications.
10. The training methodologies needed for training and creating the required knowledge and skills as well as of those required for refresher training and retention of knowledge and skills.
11. A post crisis evaluation tool, with a clear methodology for identifying lessons learned, documenting them and implementation of the necessary changes (including an evaluation of the effectiveness of the implementation).
12. Improvements identified for current Incident Management tools, in order to improve their response and usage in healthcare emergency sector, and incorporate the findings of the previous points.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

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

Expected impact:
This project will improve preparedness and response of heath services involved in large scale and/or cross border emergency situations, by developing a comprehensive set of tools including scenarios, technology, operating procedures, training programs, logistics tools, legal, ethical and public acceptance studies that will be applicable to the health care domain. This will combine applications at local, regional, cross border and international levels.

Topic SEC-2013.4.1-5 Preparing societies to cope with large scale and/or cross border crisis and disasters – Coordination and Support Action (Supporting Action)

Description of topic:
Large scale, cross-borders hazards and/or cross-border disasters (natural or manmade) directly affect the citizens who are at the same time also those who will react first to respond to their needs as well as to those of their peers. Preparing societies and the population to cope with crisis and disasters including building community resilience through involving the population in all stages of the crisis management cycle is therefore essential. As an example, earthquake preparedness programmes demonstrated the importance of public education in reducing the number and severity of casualties as well as creating real capacities in the public.

Studies on resilience at individual level have shown, however, that people do not prepare for low probability hazards. Empowering persons as well as communities should therefore build on issues that already have people's attention. Communities will already have formed social

networks around these issues which may as well be mobilised during crisis. A starting point in community resilience is, therefore, to find out which issues are important to them and how these communities are organised into social networks.

This project aims at identifying best practices as well as creating novel tools and programmes for preparing the society to cope with crisis and disasters including building community resilience and early warning.
The project should include (not exclusively):

- Identifying the crisis and disaster scenarios where society preparedness will have the greatest impact, possibly including complex scenarios with cascading effects.
- Developing cross-hazard situational awareness and risk assessment methodologies including impact identification and prioritisation schemes with a view to reinforcing preparedness.
- Understanding behavioural responses to risks and emergencies, the way the public perceive the threat, their expectations from the authorities, their expectations from themselves and their community, their motivation to take preparedness actions. This should take into account the social and cultural context.
- It should include the risk perception of citizens regarding risks they are not usually expected to come across in their own country.
- The ability of local and national administrations to deal with residents and non-residents, especially in touristic areas/countries.
- Identifying best practices and lessons learned from existing and past community preparedness programmes.
- Creating a comprehensive approach to community preparedness, looking into different groups in the society, applying a multi hazard approach whenever possible, understanding the learning needs and styles of the community members and creating the framework for long-term preparedness processes, including training. This process has to be a participatory process with the community, as much as possible.
- Creating a sample training curriculum and tools, using different training methodologies, targeting different groups in the society to various hazards to the community.
- Preparing citizens for the types of public engagement that will be used for public messaging in crises and emergencies.
- Providing a methodology to assess the effectiveness of the training programme and to assess the level of preparedness of the community. The project should include a pilot project and indicators, to demonstrate the effectiveness of the tools created.

Funding schemes: Coordination and Support Action (Supporting Action)

Expected impact:
This project should create reliable methodologies to effectively prepare the community to encounter and build resilience to a large scale, cross-hazard and/or cross border crisis and disaster situation, the methodology to assess the level of the community's preparedness and the tools to effectively train and retrain the community.

Topic SEC-2013.4.1-6 Preparedness for and management of large scale forest fires - Integration Project

Description of topic:
Large scale forest fires 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 and air fighting among others. These tools needs to be adapted to the reality of people living in what used to be only forest, which 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. Proposers should also take into account the possible environmental impacts (e.g. contamination of water) of the chemicals used by fire fighters.

Some critical infrastructures should be taken into account when they are directly affected by large scale forest fires (highways, energy grids, pipelines). Specific urban fires or fires that affect only critical infrastructures or industrial facilities should not be targeted.

Possible areas to be addressed in research:

(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 that should be considered:

(i) Transport (highways and railways going through forests)
(ii) Energy supply (High voltage grids/pipelines in forest areas)

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, a special emphasis should be given to the multi-cultural and linguistic nature of the European continent, also in terms of public behavioural models (cascading environmental/social impacts)

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.

Area 10.4.2 Response

Topic SEC-2013.4.2-1 Fast rescue of disaster surviving victims: Simulation of and situation awareness during structural collapses including detection of survivors and survival spaces – Integration Project

Description of topic:
The overall objective is to decrease the time to rescue surviving victims after a major disaster, whether it is due to natural or man-made causes.

More particularly wide-area situation awareness and survivors location solutions should be developed for rescue teams (first responders), during structural collapses. There is a specific need for a deeper understanding and analysis of typical scenarios of structures failures (collapsed buildings) and their damages depending on current and expected building materials and methods (e.g. reinforced concrete, framework of steel or reinforced concrete, glass constructions). In addition there is a big need to get an overall picture of trapped persons in collapsed buildings (to avoid a long search for survivors centimetre by centimetre in the whole destruction site).

Further, development of new rescue and recovery methods and devices which correspond to the state of the art building materials and methods (e.g. mission security systems measuring movements of debris, positioning systems, tools for cutting thick walls or girders) as well as integration of state-of-the-art location technologies (mobile, radar,…) should be carried out. These technologies, methods and devices should provide capabilities for simulation, location, detection and situational awareness during structural collapses, including fast detection of survivors, survival spaces and rescue of disaster victims. Hereto, various data sources should be harnessed that provide information about the building before and after its collapse, e.g. blue prints, satellite pictures, maps and real-time location information (integrated as coordinates on maps), photos, user-input and 3D laser scanners.

The project could also consider other disaster situations (like for example flooding, earthquake, fire, explosion…) where fast rescue response is crucial for the surviving victims.

Developments proposed in the project should be based on clearly identified end-users requirements. It should include field trials in simulated and real conditions, testing and validation activities.

The final solutions developed in the projects should be ideally:

- Mobile, quick and reliable (providing information on trapped persons in accuracy of few meters within a couple of minutes);
- Providing a clear added value to rescue teams decision making;
- Communicating and based on input information/data easily available (pictures form the scene for example);
- Ergonomic and intuitive (very simple use on the field);and
- Secured (for security and to protect data and privacy).

The proposal should take in account and integrate existing technologies and available results in particular from FP7 projects in this area.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
It is expected that the results of this integrated project will improve and contribute to shorten the time to rescue response, while saving victims and lowering the level of injuries for victims as well as rescue teams. The project will improve the general ability to rescue people from collapsed structures (buildings). It will indeed help first responders to better plan and avoid hazardous rescue operation. Key measurable indicators will demonstrate the expected impact**.**

It is also expected a better harmonisation of the response, by common procedures, tools and methods across borders, as well as solid training of the first responders to the new solutions.

Examples for possible research outcomes:
− Linking the actual measured data with existing building plans, real-time warning and connection of a 3D laser scanner to identify debris
− Development of a 3D modelling of the mission's place
− Development of standards and guidelines

Area 10.4.3 Recovery

Topic SEC-2013.4.3-1 Shaping immediate relief action in line with the goals of development co-operation in post crisis / post conflict societies to maintain stability – Capability Project

Description of topic:
The EU's holistic approach recognises the need for immediate action in crisis/conflict situations as well as the (longer-term) need to stabilise the situation and ensure security of civil society after crisis/conflict.

Thereby development cooperation, in the field of health and education, plays a crucial role to maintain and create societal security and stability, thus avoiding the relapse into insecurity. The EU already has operational funding in place via the Instrument for Stability which aims at establishing (or re-establishing) conditions essential to the proper implementation of the EU's development policies and equally through funds managed by the Directorate-General for Humanitarian Aid and Civil Protection.

Research work to be funded under this topic should support these activities; specifically the interactions between the immediate crisis/conflict relieve action, with the goals of the longer-term development co-operation. Of specific importance is the identification of immediate actions that might impede the longer-term goals. Lessons learned and further recommendations need to be developed to help policy makers and those defining relieve/rescue immediate actions to shape the crisis management activities to ensure security.

European technology, especially in field-based informatics and telecommunications, is highly developed and of particular relevance in this area. Applications for data capture in remote areas and from mobile stations can be key in monitoring emergent situations and planning rapid response. European technology to detect and rapidly respond to unusual or rare pathogens can be critical in isolating and containing diseases of pandemic potential. For example, critical information can be obtained through these technologies in situations where access to remote areas is a challenge. Adaptation of such technologies beyond the state of the art to the specific situation of post crisis/post conflict should be analysed.

The proposal should take into account technologies and results of FP7 and national projects in Social Sciences and Humanities and in other areas.

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

Expected impact:
The work should start by a study of the most important relieve actions by the EU and by the EU Member States as well as non-EU actions, in recent crisis/conflict situations. The actions thereby taken should be mapped against a) the immediate effectiveness, and b) its longer-term impact on the society/population. Beyond state of the art technologies should be tested. A 'lessons-learned' based 'do and don't' should be presented and disseminated to those concerned (planners, policy makers etc.).

Area 10.4.4 CBRN response

Topic SEC-2013.4.4-1 Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination - Integration Project

Description of topic:
Research and activities in order to identify, trace and monitoring of a large number of people in case of a massive CBRN (Chemical, Biological, Radiological or Nuclear) contamination is needed. This should allow to rapidly identify persons at risk (potentially contaminated) with

the view to treat them in a rapid and appropriate way, including methods to differentiate between contaminated or not contaminated persons on-site or in hospital zones.
In this context, the objective of this project is to integrate existing tools and procedures along with the development of novel solutions in order to (non exhaustive list):

- Rapidly identify and assess the risk of contamination of persons exposed or that have been in contact with possible source of contamination (by a Chemical, Biological or Radiological contaminant).
- Rapidly identify and assess 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 and triage standard operational procedures for hospitalisation and admission to intensive care units (or other specific units) based on the risk assessment data.

Proposals should try to cover as much as possible listed needs for C, B and/or RN and take into account the account technologies and results of FP7 and national projects as well as the ongoing EU policy developments.

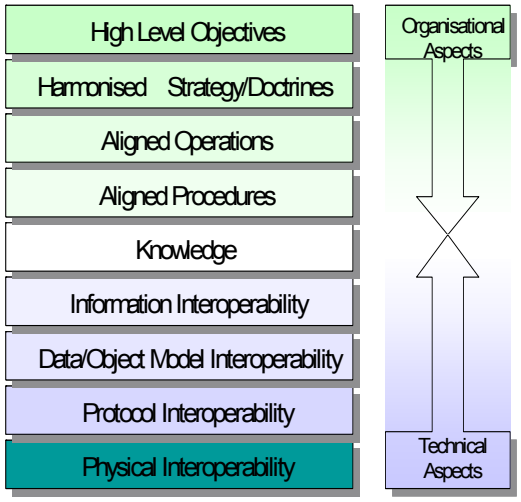
The Ethical implications and social acceptance of the proposed solution(s) have to be addressed specifically.
Funding schemes: Collaborative Project (large scale integrating project)

Expected impact: Breakthrough on detection and monitoring capabilities of contaminated persons (C, B and/or RN) to the benefit of first responders, civil protection and public health services. In addition, this project is expected to provide a new integrated, interoperable and centralised system approach involving stakeholders in case of a mass CBRN contamination

Activity 10.5 SECURITY SYSTEMS INTEGRATION, INTERCONNECTIVITY AND INTEROPERABILITY

Activities 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 targeted to solving practical interoperability, intercommunication and interconnection issues in the security field, with a holistic and cross-cutting approach, while ensuring reliability, confidentiality and integrity of information.



Its focus is to target the interoperability requirements of horizontal or enabling technologies, processes or other layers of the interoperability stack, that can be applied to several different scenarios, as those covered by mission areas 1 to 4.

Important elements in this activity will be: communication and interaction among different organizations and nations; relationship among end-user's processes, training and technological issues; Interactions between technological and organizational factors; interoperability between information and command functions; interoperability among different equipment deployed in security incidents.

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

Area 10.5.1 Information management

Topic SEC-2013.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities – Capability Project

Description of topic:
The first objective is to create a pan-European inventory of:

- past critical events/disasters and their consequence including the time dimension and the response given in terms of means used, costs, etc. again with the time dimension;
- information about the data sets, the daily information management tools and processes, the integration into crisis management procedures and the information systems used by first responders and police authorities in disaster and crisis management procedures; and
- how crisis and emergency management services are deployed in terms of organisation business model: in-house, outsourced, etc., and how each approach affects the service.

The final objective is to derive from this collection of information a taxonomy and a network enabled communication system concept ("common information space") to be used at European level with a view to enable collaboration processes and exploitation of information from different sources and across borders. A particular effort will be put into identification of new possible emergency and crisis management models. For instance, should be considered: multi-agency systems, i.e. systems deployed to provide service to same-purpose, different geographic area responsibility agencies so they can benefit from cost sharing while maintaining their service independence.

In addition, the research should cover regulatory aspects as well as restrictions identified for emergency management practices and tools (laws, social practices and culture, etc.) that should be taken by European industry in the field of study, in order to adapt its offering to each member state restrictions. In addition, service provisioning aspects should be covered (outsourced services, outsourced technologies, etc.)

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

Expected impact:
It is expected to allow for interoperability at operational level (multi-agency, cross-border guidance capabilities) and new ways of service provision in the field of public safety and crisis management activities. It is also expected that research should start standardisation activities in this area and create a level playing field for industry to facilitate the development of an EU market.

Topic SEC-2013.5.1-2 Audio and voice analysis, speaker identification for security applications – Integration Project

Description of topic:
In the course of investigations, numerous audio data are at the disposal of law enforcement agencies (LEA). Terrorist threat or attack claim, hostage takings, demand of ransom, wire-tap during crime investigations, audio records in busy/noisy environment are some examples of the situations LEA can face.

The objective of this topic is to improve the technical capabilities to identify individuals through the speaker's voice recognition. There are numerous research issues at stake such as: better recording devices, taking into account new media, new innovative analysis algorithms, real time audio data analysis, language recognition, speaker identification and management of large audio databases. The project should propose and integrate innovative algorithms and solutions for speaker recognition that will fully comply with ethics and privacy EU regulations. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have also to be taken into account in a comprehensive and thorough manner.

Proposers for this topic should look for an enhanced SME participation as described in Part 1 of the work programme.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact:
It is expected to extend the capability of LEA with innovative and operational tools and solutions in this area. It should pave the way to standardisation in this area as well as validation and certification of the proposed solution, and to facilitate level playing field for industry in this sector as well as the creation of a European market.

Area 10.5.2 Secure communications

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

Area 10.5.3 Interoperability

Topic SEC-2013.5.3-1 Definition of interoperability specifications for information and meta-data exchange amongst sensors and control systems – Capability Project

Description of topic:
Command and control technological systems are nowadays at the core of the C3 (command, control and communications) human function at most complex operations, as a key element for augmenting and assisting command in the decision making process. These systems depend upon the reception of raw data or pre-processed information transmitted from multiple sensors and sources.

However, the efficient integration of information from these sources can be extremely challenging, technologically complex and time consuming, as well as very expensive. This forces the use of specifically tailored integrated solutions, for which the exchange of components from different vendors or the integration of new ones can be very difficult.

Reasons for this are factors such as: the increased number of joint operations, where information is sent by first responders from different nationalities or organizations, or just using different technologies; the wide diversity in the nature of the possible sources and signals, the growing number of possible sensors to be used, their nature (e.g.: autonomous or networked, simple or intelligent); differences in their environment; time constraints for the response; or just the speed of technological evolution. All these have to be considered.

The task is, first, to describe and create an as large as possible inventory of representative real life examples of sensors, control systems, communications, and architectures for different scenarios in the security field. A second task is to define a taxonomy and propose a framework that could evolve into a standard specification for interoperability (physical, electrical, data, etc.) between sensors or other sources, and command and control systems, with the aim of helping the development of a European market in this field. The project should also specify the framework in order to allow future devices interoperability.

The proposed framework should enable effective exchange of information between different rescue units, public safety units and crisis management information systems operating together without any special technical prearrangements, e.g. in case of activities within the European civil protection cooperation framework or when participating in the international relief operations.

The definition of common interfaces, data structures and procedures should take into consideration both the functional and the operational requirements for their use in the security field enabling the exchange of data, as well as security requirements and legal constraints.

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

Expected impact:
To start standardisation activities in this area which would help:
- to have common specifications for similar functions;
- to allow for validation and certification of sensors and sensor systems;
- to facilitate interoperability of sensors and sensor's systems; and
- to create a level playing field for industry to facilitate an EU market.

Topic SEC-2013.5.3-2 Testing the interoperability of maritime surveillance systems – Pre-Operation Validation

Description of topic:
Legitimate and unlawful activities developing in ports, coastal waters and high seas are deeply influenced by the absence of geographical delineations; maritime security relies abundantly on a comprehensive and enhanced maritime picture of the full set of sector activities in the maritime area. Addressing security challenges developing in the European maritime domain relies therefore on the integration of maritime surveillance and on a better cross-sector and cross-border approach.

An integrated maritime surveillance over the European maritime domain would provide more effective situational awareness at sea, including for security and safety purposes. It would contribute to the fight against unlawful activities (e.g. drug smuggling, trafficking in human beings, irregular migration and terrorism at sea and from the sea). Improved situational awareness of activities, and better knowledge of maritime environment, would also enhance decision making with respect to incident management and timely interventions at sea, contributing to optimising the operational management of intervention missions dealing with security, safety and environment protection.

The EU defined its objective to set up a Common Information Sharing Environment (CISE) for the maritime domain[41]. This requires cooperation across sectors (i.e. border control, customs, general law enforcement, defence, control of maritime pollution and marine environment, fisheries control, as well as the economic interests of the EU) and borders.

Several pilot projects (such as MARSUNO and BlueMassMed (European Commission Directorate-General for Maritime Affairs and Fisheries as well as BlueBelt and e-Maritime (European Commission Directorate-General for Mobility and Transport)), selected components of EUROSUR (European Commission Directorate-General for Home Affairs), and operational initiatives, like MARSUR (European Defence Agency) and SUCBAS (Baltic Sea Navies), have demonstrated the need to shift from the conventional "*need to know*" approach towards a cross-sectorial and cross-border "*need and responsibility to share*".

The projects mentioned above have already proven cost-effective approaches for trans-sectoral data sharing. What remains as technological challenge is the cross-sectoral dimension where legal constraints have to be implemented by secure and selective information exchange, with functionalities agreed and trusted by all end-users (access right policies, information exchange security policies, information services). Indeed, even though authorities would be connected and exchange information within CISE, be it at the Member State's agency or individual level, they must always act according to the person's agency of origins duties, rights and competences. The complexity of these functionalities relates therefore to the wide diversity of user communities, each of them having specific kind of data and rules for handling them, the heterogeneity of the current legal framework, and the high number of institutional actors.

The anticipated implementation of CISE at the full EU/EEA scale is estimated to eventually correspond to a de-centralized interoperable and trusted cross-sectoral data exchange environment between over 400 relevant public authorities and administrations, whose information system, and data, widely differ in terms of architecture, capability and

[41] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/genaff/122177.pdf

functionality. Developments in this area imply the achievement of a higher level of integration of systems and components in a heterogeneous environment.

Interoperability, both technical and functional (i.e. the ability of systems to provide services to, and accept services from, other systems and to use the services so exchanged to enable them to effectively operate together), is a must for the coherent development of operational information exchange capabilities in a trans-national environment. For each system efforts would be required both at the internal level, setting homogeneous requirements for handling and display of information, and at the external level, facilitating the interfacing of systems.

The aim of this POV is to test and validate the CISE concept (surveillance standard), under realistic operational and formal conditions, for the cross sectorial data exchange at EU/EEA level in a test-bed connecting the systems of only a subset of the concerned EU/EEA public authorities. The pre-operational validation of this tested solution is expected to prepare the way towards the later implementation on a larger scale across Europe. The POV shall be organised while respecting the Treaty principles, the competition rules and the specific requirements indicated in the Appendix.

The proposed topic shall be seen in line with the EU Integrated Maritime Policy and the EU Internal Security Strategy. It aims at stimulating national authorities and the industry to converge for the development and test of interoperable information sharing tools, in order to validate solutions for cross-sector and cross-border information exchange.

The topic 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.

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 developments towards a prototype for CISE, and the testing of the proposed solutions against a set of jointly defined concepts of operations and performance criteria.

In this scheme, in order to support cooperation between public authorities participating in the preparation and management of the POV, the joint POV procurement for the development, test and validation of the network of systems will be accompanied by a coordination and support action (CSA). The CSA support aims to enable participating authorities to prepare, define and jointly (in coordination with other relevant EU organisations, as appropriate) implement the POV procurement, and later jointly assess its outcome.

The nature and the objectives of this indirect action are such that it requires the participation of at least three independent public authorities in charge of maritime surveillance in different sectors (at local, regional, national or supra-national levels), each established in a different Member State or Associated State. However, the nature of the challenge is such that a larger number of participants are encouraged.

Although the application focus of the action is to remain civil, at least one of these participating authorities should belong to the defence community in order to ensure a comprehensive approach in the sharing of defence information useful to the civilian tasks at sea, in order to avoid duplications. Other stakeholders (e.g. EU agencies), may participate in addition, if their participation is well justified and adds value to the action, e.g. if:

a. they represent an authority or a regulatory body with responsibility in some area affected by the use of a particular technology,
b. their support is required in order to facilitate the technical, administrative, financial or managerial procedures for which national authorities are limited by their respective national regulation.

The participating authorities should test the exchange of information through surveillance services (testing CISE standard) in order to obtain the best situational awareness picture available, for their own mission, based on multi-sectoral and cross-border sharing at least between their systems and with EU systems like SafeSeaNet, MARSUR, EUROSUR, Cleanseanet, Emodnet and VMS.

The overall project duration is expected to be between 18 and 27 months.

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

In the context of the European Integrated Maritime Policy and of the EU Internal Security Strategy, this CP-CSA is to conduct pre-operational validation of tools for the common information sharing environment at sea at EU/EEA level via the competitive development testing and assessment of a potential solution.

The specific objective of this project is to have a test-bed network of systems connecting participating public authorities developed for cross sectoral data exchange and tested in particular to assess, in the context of CISE:

- the technical feasibility of option(s) for the Common Information Sharing Environment (CISE) at sea;
- the identification of technological alternatives for the achievement of the set of user-defined operational objectives;
- the demonstration that there are existing innovative solutions (services) which provide the required capabilities;
- the feasibility of the integration of the proposed solution, taking into consideration the limitations imposed by the existing surveillance systems;
- the performance under realistic operational and formal conditions of the test bed developed;
- the cost-benefit ratio of the option(s) tested;
- the identification of the maturity level showed by the solution(s) 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 tools;
- the evaluation of the experimentation results promoting their widening to future solutions; and
- the definition of advisable technical management structure for CISE.

As part of the project activities, the industry shall be called to provide solutions to be tested and validated according to the concept developed by the consortium participants based on CISE definitions and rules provided by the European Commission in due time before testing and validation. In order to guarantee an independent and reliable validation process of the proposed solutions, a mechanism has to be enabled that supports the activity of the different actors throughout a series of steps.

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 CISE. It should build on the specifications being set by the relevant expert group.[42] This can also be seen as a follow up of the pilot projects "Marsuno" and "BlueMassMed" where the needs of Member States for higher level of interoperability have been affirmed.

The challenge is to undertake the proper cooperative R&D work and validate it with a sufficiently representative set of institutional actors. Public sector requirements for interoperability, information security and data portability will therefore have to be considered across the participating authorities (and sectors).

Participating authorities are expected to present their cooperative plan (access to their surveillance services) for definition of the later phases, in coordination with other relevant EU organizations (where appropriate).

The consortium shall set up appropriate IPR rules with a view to allow authorities of non participating Member States/Associated Countries (and European authorities) to make full use of the developed technologies.

For these reasons, in this CSA a strategy shall be put in place for:
- Identification of elements requiring new R&D that should be tested and validated in cooperation[43];
- Definition of an action plan, setting scenarios and issues for concrete implementation of activities;
- Establishment of modalities and procedures for POV evaluation and monitoring (common evaluation criteria and implementation methods);
- Drafting a preliminary CISE IPR strategy for the (expected) outcome of the Call for Tender, 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 Needs Analysis Document and a Validation Strategy Document, including a practical Exercise Plan for the actual development and 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

[42] See: "*Member States Expert Group for Integrated Maritime Surveillance*" https://webgate.ec.europa.eu/maritimeforum/content/2657

[43] A pre-study on the landscape of existing situation of systems and projects is expected to be completed by June 2012. A study of the technical definition of CISE environment will be launched in July 2012 and technical requirements are expected to be ready mid 2013 well before testing and validation.

competitive tenders, and for selection/award of the tender. Such call shall be defined in such a way that it respects the Treaty principles and the specific requirements in the 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 implementation and testing).

In this phase the providers of solutions to be implemented and tested will execute their work according to the prescription of the action plan, working under the supervision of the concerned participating public authorities, having the network of systems tested by them for cross sectoral data exchange under realistic operational and formal conditions.

The Implementation Plan is expected to be contracted during 2014-2015 and implemented in 2015. Operational testing of the developed network environment should last at least 6 months.

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

In this phase, which will conclude the overall validation, participating public authorities, in coordination with other relevant EU organizations, will conduct a thorough assessment of the performance of the network of systems, as demonstrated in the testing exercises of phase 2, against the set of jointly defined performance criteria. The aim will be to verify its fitness for purpose in terms of implementation of the CISE concept, with a view to a later potential conversion of the systems tested into services. 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 is expected to be implemented in the first half of 2016.
For implementing this CP-CSA, different constellations for joint validation[44] are allowed, such as for example common validation entity[45], lead authority[46] and piggy-backing[47] constellations.

EU CONTRIBUTION

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

[44] "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.

[45] 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. This entity shall be integrated among the project beneficiaries in equivalent conditions in terms of rights and obligations, and support the decision process, facilitating the development of a validation strategy and the arrangements for launching a competitive call for the demonstration of surveillance capabilities.

[46] 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.

[47] 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).

- 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*"[48]) (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).

It is clear from the above that, in addition to the EU financial support to phase 2, participants shall contribute directly to the research and technological development activities involved in the testing of new solutions. This contribution of the participants to phase 2 can be in kind (e.g. personnel, premises, systems and services).

Expected impact:

This CSA-CP is expected to significantly contribute to the implementation of CISE.

Enhanced maritime awareness will help ensuring more secure, safer and cleaner seas. Search and rescue authorities will make use of better information when people's lives are in danger at sea. Coast Guards, police and navies may better share information to better prevent and combat all kinds of illegal activities at sea or to protect merchant ships, fishing and pleasure boats from all kind of threats. Environmental and pollution prevention and response authorities may better share information with maritime traffic or control authorities, allowing to better prevent, intercept or clean-up pollution at sea.

The commitment (and credibility) of relevant participating public authorities across different sectors is an essential requirements to ensure the later take up of the proposed solution at the EU scale. The output of the project is expected to be a validated technical and operational reference framework, a “test bench” to be used for the setting up of future interoperable systems at a larger scale. At the end of the project, the participating authorities should have obtained clear evidence of the cost-efficiency of the approach. The consolidation of requirements and joint procurement is expected to lead to future reduced costs.

The project is 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.

This project is expected to imply a relevant standardisation component. Common interfaces, data structures and procedures would be necessary for the exchange of data, making security information available where it is needed, while respecting legal and regulatory constraints. Standard procedures are expected to be set up to improve the communications between heterogeneous systems (from operational and technical standpoints).

[48] 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

Impact will be measured essentially in terms of fitness for purpose in the context of CISE. However, the expected impact goes beyond purely technical aspects and covers aspects related with the industrial market of security solutions. Through the execution of the project, participants are expected to verify and optimise their technological choices. Technology providers would increase their understanding of modern operational requirements, with adaptation of existing technologies, and novel research and development, to address the challenges of maritime surveillance, thus increasing their competitiveness. The project has the potential to create important market opportunities worldwide for the European industry and establish a clear leadership in this area.

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[49] 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**[50] **services contract**[51].
- More than 75% of the EU contribution is expected to fund Phase 2 (Preparatory Work and Execution Phase).
- **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.
- **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[52].

[49] 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.

[50] 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.

[51] 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.

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

- In respect of the Treaty principles the public purchasers shall ensure **EU wide publication** for the POV call for tender[53] 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.
- 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), and the institutions of the European Union, 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 maritime 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. 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[54] 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 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, if appropriate, the format of the intermediate evaluations after the solution design and prototype development stages that progressively select organisations with the best competing solutions.

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

[54] 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.

Area 10.5.4 Standardisation

Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products – Capability Project

Description of topic:
Today security equipment and systems are very diverse in technology, concept of operations, application areas and performance. Similar security products are difficult to compare in terms of performances, accuracy, usage, trust they could deserve and validation of the functionalities. Currently, there are very few harmonised certification procedures in Europe applicable and recognised similarly in each Member State.

Lacking a harmonised approach in the EU and Associated Countries across application areas (e.g. critical infrastructure, crisis management) means that incentives for development by the European security systems industry are suboptimal. Mechanisms to independently evaluate security products, on a scientifically valid and statistically reliable basis are sought for development and implementation across the EU.

The task is to study if and how existing evaluation and certification schemes (such as Common Criteria - ISO 15408, and other relevant standards) could be used and possibly further developed/enhanced/adapted/integrated for the assessment and certification of products used for physical security of people and infrastructures. If finally applicable, this should be validated by experiments on some different product types and different methods (e.g. anti-spoofing methods...). The identification of the correct standardisation bodies (and to some extends national standardisation bodies) is a pre requisite. Outputs of the project should feed the identified standardisation bodies with proposals for new work items.

A legal study should also be carried out to analyse ethical and privacy issues as well as existing or upcoming regulations. Finally, the involvement of a few Data Protection Authorities (DPA) (for example through Advisory Groups) is highly desirable, in order to facilitate the emergence of an EU–wide security certification process, the value of which would be acknowledged by all DPAs.

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

Expected impact:
The project is expected to facilitate a harmonised playing field for the security industry and to enhance the trust of the professional users and thereby of the EU citizen in security products. A clear roadmap with identified milestones and a definition of coverage for the certification scheme is also expected. The provision of accreditation schemes would provide grounds for confidence in the reliability of the judgements on which the original certificates were based by requiring that the Accreditation Bodies should meet high and consistent standards. This should also lead to an evolution of the current EU regulations, for a wide acknowledgement and harmonisation of certification schemes and mutual recognition across all Member States.

Activity 10.6 SECURITY AND SOCIETY

Activities 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 the rights to privacy and data protection, freedom of expression and association, good governance and 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 and civil society organisations. 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 bring about 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 mission-oriented approach, 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 in relation to societal impacts.

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 requirements for interoperability; 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-2013.6.1-1 The impact of social media in emergencies – Capability Project

Description of topic:
The impact of social media in emergencies and their impact on public feelings of security and insecurity are poorly understood. Research is needed on various facets of the growing importance of social media in situations of societal emergencies or when facing threats to citizen security as in civil protection situations.

Social media play a crucial role in any event locally, nationally and internationally. There is little systematic research based knowledge about what role they play in emergency situations. Social media are also vehicles for story telling and rumour spreading of vast proportions in disasters with many uncertainties and complex interactions. Research is therefore needed on the consequences of the new pattern that social media may very quickly provide information (reliable or unreliable) on fast moving developments.

Research may focus on the following issues:

- How and when do social media contribute to the general understanding of what has happened, the reasons why it has happened?
- How do people react, what might be the consequences, what reactions are/should be chosen by the authorities?
- Under what circumstances do the social media play a social responsible role or an irresponsible role that aggravates the critical situation?
- What is the difference between the different types of social media?

Social media becomes a complicating influence in crises unless new tools and methods are developed to meet this challenge. New tools which can be applied in different scenarios are also needed to reduce potential information overload among incident commanders.

Involvement of social network providers is encouraged. Proposers for this topic should also look for an enhanced SME participation as described in Part 1 of the work programme.

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

Expected impact:
Stakeholders should get a better understanding of the impact of social media before, during and after emergencies, as this new dimension adds uncertainty and complexity. This research should lead to better emergency management systems and crisis management tools in terms of information gathering, information filtering, intelligence extraction and incident identification applied in different scenarios.

Topic SEC-2013.6.1-2 Varying forms of terrorism – Capability Project

Description of topic:
Research on terrorism and violent radicalisation process and violence promoting extremism has tended to concentrate on groups of people with specific attitude and action patterns. We know less about what social, educational and cultural and psychological factors and attitudes that may lead to individual fascinations with extreme violent ideas, and what would bring a single person from ideas to action. We also have limited knowledge about how such a potentially violent situation can be uncovered, hindered, mitigated, anticipated and prevented. There is also a lack of information on the main stages radicalised people go through and their timeframe. We must assume that answers to these highly complex questions will change over time and across contexts given the impacts of globalisation, rapidly advancing social media, and other relevant trends.

Furthermore, Europe has experienced forms of right wing, left wing and anarchist violent extremism and terrorism that warrant closer analysis and understanding.

Research may focus on the following issues:

Radicalisation Processes and Paths – ideas and actions
- What are the psychological and social processes of radicalisation that lead to someone becoming committed to violent extremism?
- What can be learnt about the people involved in a radicalisation process?
- What are the stages of their radicalisation process?
- What are the processes and stages of self-radicalisation that lead to a solo person committed to acts of violent extremism?
- What relationship is there between radicalisation processes and violent ideologies, methods, intentions and targets?
- What would bring a person from extreme violent ideas to violent action?

Influencing Factors (or Root Causes)
What factors increase or decrease the risks of individual or group radicalisation and of self-radicalisation? For example, the role of:
- upbringing, school;
- family and social environment;
- psychosocial factors (including group dynamics);
- religion and ideology;

- the internet and social media;
- easy access to weapons and explosives;
- socio-economic factors; and
- political and legal factors.

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

Expected impact:
The research will help in identifying root causes, and counter measures to assist the work of national authorities as well as local communities, and to strengthen the societal resilience.

National and local communities can better prevent, prepare for and protect themselves against such varying forms of deadly violence. For example:
- New equipments and systems can support these objectives.
- Practices, processes, procedures and methodologies can be improved for the benefit of the citizen.
- Authorities can better manage information and communication with the public.

The research and the usable results should consider fundamental rights protection, comparative studies of international laws, ethical and societal impacts, in particular with relevance to EU anti-terrorism policies.

Topic SEC-2013.6.1-3 Trafficking in Human Beings: analysis of criminal networks for more effective counter-trafficking – Coordination and Support Action (Supporting Action)

Description of topic:
Trafficking in human beings (THB) is one of the largest criminal industries in the world. While research on this phenomenon has increased in recent years, to date the focus has been primarily on victims and survivors of the crime and little is known about the perpetrators.

Serious efforts in addressing THB require a clear understanding of current trends not only in regards to victims, but also regarding traffickers, trafficking networks, their modus operandi, their travel routes and the different forms of THB committed by them. To develop effective strategies to combat the crime of human trafficking, it is necessary to better understand the organisational structure of those participating in the trafficking business.

Offenders quickly adapt and improve their techniques, routes and methods in response to law enforcement strategies against THB. The clandestine nature of activities and the use of illegal channels are increasingly prevalent features. Members of the trafficking organisations are located in origin, transit and destination countries; therefore they can easily react to new market situations. For effective counter-trafficking policies and activities, it is imperative to equip relevant actors with detailed and up-to-date information.

The project should include at least the active participation of one authority officially in charge of addressing trafficking in human beings at the national or European level.

Funding schemes: Coordination and Support Action (Supporting Action)

Expected impact:
Increased information on offenders is anticipated to contribute to better identification of vulnerable groups in danger of being trafficked. It is a real challenge to know how to deal with those who become part of trafficking networks, who sometimes may have been in the first place victims themselves. Understanding the structure and nature of social relationships within trafficking organisations is expected to provide stakeholders with important information to combat/prevent the recruitment of victims through other victims and to disrupt the business of trafficking.

Research actions to be conducted should be complementary to on-going EU and national projects and activities (e.g. CAPER, activities of the SSH theme, EUROPOL, etc.).

Area 10.6.2 Organisational requirement 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. Fulfilment of the ambitions of the Solidarity Clause of the Lisbon Treaty and implementation of the Internal Security Strategy require such organisational and cultural compatibility across Member States.

Topic SEC-2013.6.2-1 Facilitators for assistance among EU Member States in emergencies in the EU – Capability Project or Coordination and Support Action (Coordinating Action)

Description of topic:
The Solidarity Clause of the Lisbon Treaty suggests ambitious objectives for mutual assistance among EU Member States in emergencies in European territory. The organisational structures and cultures of public agencies responsible for such mutual assistance efforts need to be prepared to provide and to receive such assistance from other Member States – EU Host Nation Support Guidelines should be taken into account. Research is needed on the organisational components and process elements that may facilitate or hinder such compatibility among the responsible agencies and supporting actors in cooperating Member States. Such joint arrangements must be cost effective and usable. They must also be acceptable to engage stakeholders, including supporting actors, such as businesses and civil organisations. Without better knowledge about institutional arrangements and organisational cultures affecting such efforts, these will not become effective in support of citizen security.

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

Expected impact:
The new knowledge and/or technologies will serve as input in the design of new arrangements to deal with mutual assistance in future emergencies in the EU. The coherence and effectiveness of European actions will be strengthened.

Area 10.6.3 Foresight, scenarios and security as 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.

Security is a concept with many interpretations. Research is needed on the various meanings, perceptions and practices of security in the Union. Europe's security needs do not only rise and fall in relation to concrete threats. They change as a result of technological advances and social evolution. How does European security research in fact contribute to the real and the sensed enhancement of security for the citizens?

Topic SEC-2013.6.3-1 Horizon scanning and foresight for security research and innovation – Coordination and Support Action (Coordinating Action)

Description of topic:
Up to now a considerable number of security related foresight activities have been funded in the FP 7 security theme. It is therefore timely to draw upon the results of these, and to develop a consistent 'horizon scanning' in security to deal with expectations about future developments in a rational manner. Foresights studies produce expectations about mid-term and long-term trends, while scanning can also look at short-term evidence for emerging risks. These expectations tend to change accidently, caused by external events. So for reliable long-term trend analysis it is also necessary to understand the dynamics in these changes.

Horizon scanning and foresight activities will address social needs, as well as scientific capabilities and technical solutions. For each scanning activity different sources need to be included. The mapping of existing security related foresight studies and internet data in general can be used for both activities.

Transparent, public knowledge about long-term trends and drivers is very important for the efficiency of the European security research innovation system. Each stakeholder has its own expectation about future trends and behaves in accordance to this expectation. Misleading expectation can cause wrong investments, wrong political strategies or other expensive mistakes. To have reliable information about future social needs and possible technological solutions is a win-win situation for all stakeholders of the security innovation system.

It is important to link process models of the impacts of identified risks to decision support frameworks so as to ensure evidence based decision making.

Proposers are strongly encouraged to develop solutions in compliance with European societal values, including privacy issues and fundamental rights.

The visibility and the take up of security research results at stakeholder level, especially focusing on the end users, still have to be improved.

Research activities to be conducted should draw upon results of and be complementary to FP7 and national activities funded in this area (such as the projects SIAM, DESSI, FORESEC, FOCUS, FESTOS and ETTIS).

Funding schemes: Coordination and Support Action (Coordinating Action)

Expected impact:
The results should provide more effective information into foresight for political agenda setting and also provide a better understanding of the new and upcoming technologies and long-term trends, leading to the strategic planning into security issues of relevant stakeholders.

Topic SEC-2013.6.3-2 The evolving concept of security – Coordination and Support Action (Coordinating Action)

Description of topic:
Security is a concept with many interpretations. Yet, it is a core element in the common aim to build a more secure Union, as envisioned in the Internal Security Strategy. Research is needed on the various meanings, perceptions, legal comparative laws, and practices of security in the Union. Europe's security needs do not only rise and fall in relation to concrete threats. They change as a result of technological advances and social evolution.

Security is a concept that is used about many types of situations and can be seen as a given, but in reality it varies a lot according to the situation, the persons, the experience, age and gender. Its meaning may be provoked or eased by media, by surveillance, police and by legal factors.

Research in this area will document and analyse the evolution of security thinking and practices as the result of multiple factors: social values, technological innovation, politics, legal, economics, etc. This will contribute to a more complete understanding of the pros and cons of measures to take in order to enhance Europe's security.

Research activities to be conducted should draw upon results of and be complementary to previous FP7 and national activities funded in this area.

Funding schemes: Coordination and Support Action (Coordinating Action)

Expected impact:
Both perceptions of threat and the measures that are taken are directly influenced by a shared concept of security. The evolution of the concept can be expected to have a direct impact on both of these areas. Proposals should directly address these challenges. Among potential impacts of the research should be changes in the working parameters of various types of security end-users. How does the evolution in the concept of security impact the way police, border guards, first-responders, social services, NGOs and others do their work, understand threat, and assess the risks connected to their work.

Area 10.6.4 Security economics

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

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 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-2013.6.5-1 Synthesis of results and reviewing of ethics, legal and justice activities in Security research in FP7 – Coordination and Support Action (Coordinating Action)

Description of topic:
The action will define the strategic roadmap required for future research projects in the area of ethics and justice. This roadmapping activity should take into account relevant completed and ongoing work (notably projects in this area such as PRISMS, SURPRISE, DETECTER, INEX, SMART, SAPIENT, ADDPRIV). It shall lay out in a coherent and clear manner the further research work required. It will assess the relevant factual and political situation and trends.

Funding schemes: Coordination and Support Action (Coordinating Action)

Expected impact:
The action will provide a solid basis for sequencing and describing research tasks to be called for in the future.

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 Member States and Associated Countries as well as between relevant organisations at the European level. All this will contribute to the overall impact of the Security theme by making it more effective and efficient, will raise the innovation level in the security domain and will achieve increasingly harmonised implementation approaches.

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-2013.7.2-1 Open topic for Small and Medium Enterprises: "Solutions for frequent petty crimes that are of high impact to local communities and citizens" – Capability Project

Description:

This specific open topic aims at improving security in local communities and for citizens.

Work funded under this topic should address insecurities towards local communities (citizens and businesses). Crime such as theft, extortion, fraud, etc poses a serious threat to their well being. High crime rates negatively impact the surrounding commercial and social environment which makes communities less resilient and less likely to receive inward investment. Existing communities do not prosper and are reluctant to expand resulting in a downward spiral.

Furthermore, work funded under this topic should identify and then look into solutions for frequent but low-intensity sources of insecurity that nevertheless have high impact on communities and citizens.

Project(s) to be funded are expected to be innovative research and development work, leading to low cost technology based solutions, meeting the needs and financial expectations of 1) the communities and 2) citizens. The cost to benefit ratio of the proposed solution should be analysed against the impact of the threats.

Indicative research areas could be for instance:

1. to develop new technologies/methods to protect local business and/or citizens from theft and/or extortion and/or fraud;
2. to develop new technologies/methods for the general protection of citizens from physical violence;
3. to develop a technology method for the general protection of private ad public properties against vandalism (e.g. train/subway stations, facades/walls, cars, etc.); and
4. any other field relevant for frequent in-security situations that are of high impact to local community businesses and citizens.

This open topic should lead to projects that have strong SME participation / consortia that are led by SMEs. Projects may also support the acquisition of technologies / knowledge needed for SMEs, thus bringing together SMEs with the researcher community that are typically out of the reach of SMEs. Accordingly this Topic should help SMEs providing real solutions for real issues.

For each project/consortium, the following recommendations apply:

- at least 50% of the EU funding should go to eligible SMEs;
- small-sized projects are encouraged (up to € 1.5 million EC Funding);
- the project duration should be up to 2 years;
- small consortia (3-7 partners) are encouraged;
- SME coordinators are encouraged but they are by no means mandatory – lack of prior FP7 experience should not be seen as a handicap for an SME coordinator; and
- 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 innovative low cost solutions will be developed that reduce crime against local communities, businesses and citizens. Thereby the project(s) should be leading to demonstrable positive impacts. These solutions should offer the prospect of export of goods/services from the EU to global markets.

Area 10.7.3 Studies

Topic SEC-2013.7.3-1 Increasing the engagement of civil society in security research – Coordination and Support Action (Supporting Action)

Description of topic:
Security research engages many different stakeholders. There is a need to increase the engagement of representatives of or advocates for civil society in security research. A study is needed on how and where these organisations participate already in research activities, and what measures to increase their participation already exist elsewhere in FP7. A strategy should also be developed with concrete action steps how to increase their participation in both the shaping and the implementation of civil security research. Also, steps should be considered on how to ensure a greater understanding among civil society organisations of the potential benefits, especially with regard to societal security, of the results coming from security research activities.

Funding schemes: Coordination and Support Action (Supporting action)

Expected impact:
The outcomes should include an action plan which will help achieving a greater engagement with and involvement of civil society organisations and their advocates in EU security research in the future.

Area 10.7.4 Other coordination

Topic SEC-2013.7.4-1 Trans-national cooperation among public security research stakeholders – Coordination and Support Action (Coordinating Action)

Description of topic:
The aim of the topic is to improve coordination at European level of various national or regional networks in different security research domains (for example law enforcement, forensics, airport security, etc). Activities can concentrate on a specific core area or cover several areas.

The action should further aim to: a) exchange information on security issues in their countries and define core areas of common interest in order to prevent duplication and identify synergies, b) exchange information about research needs and latest technological developments, c) develop common strategies and mechanisms in the specific area(s), and d) explore possibilities for coordinated and/or joint activities.

Funding schemes: Coordination and Support Action (Coordinating action)

Expected impact:
It is expected to improve networking and coordination of various national/regional activities relevant to Security research at European level.

Area 10.7.5 End-users

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

Area 10.7.6 Training

Topic SEC-2013.7.6-1 Open topic for Small and Medium Enterprises: "Use of serious gaming in order to improve intelligence analysis by law enforcement agents" – Capability Project

Description of topic:
The quality of intelligence analysis depends on the analysts' skills; even though training programmes have progressed supported by e-learning, there is still room to improve the creative, reasoning skills and reflexes of the law enforcement agents. The objective is to develop gaming solutions that address the requirements of the civil security intelligence analysis community.

Research is required in two stages:

- First, to capture the way analysts have to think, using both deduction and induction, and exploiting fully their skills, knowledge, experience and creativity. The ideal analyst uses both rigorous analysis and attention to process and detail, and also imagination and the willingness and ability to make inspired guesses.
- Second, research must develop new approaches on how technology can support training and development. This stage must consider the psychological, behavioural, technical and

pedagogical issues in order to develop innovative training approaches, processes, procedures and methodologies.

For each project/consortium, the following recommendations apply:

- at least 50% of the EU funding should go to eligible SMEs;
- small-sized projects are encouraged (up to € 1.5 million EC Funding);
- the project duration should be up to 2 years;
- small consortia (3-7 partners) are encouraged;
- SME coordinators are encouraged but they are by no means mandatory – lack of prior FP7 experience should not be seen as a handicap for an SME coordinator; and
- at least one end-user should be included in the consortium.

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

Expected impact:
The objective is to develop solutions that address the requirements of the civil security intelligence analysis community. Research should go beyond E-learning and already existing virtual classroom. 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 serious gaming area.

III. IMPLEMENTATION OF CALLS

For description of the topics of the calls, please refer to section II 'Content of calls'

FP7-SEC-2013-1

- **Call identifier**: FP7-SEC-2013-1
- **Date of publication**: 10/July/2012[55]
- **Deadline**: 22/November/2012 at 17.00.00, Brussels local time[56]
- **Indicative budget**: EUR 299.33million[57]

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

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

[55] The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.
[56] The Director-General responsible may delay this deadline by up to two months.
[57] Under the condition that the draft budget for 2013 is adopted without modification by the budgetary authority.

- **Topics called**:

Activity/ Area	Topics called	Funding Schemes
Activity 10.1 Security of citizens		
Area: 10.1.1 Organised crime	Topic SEC-2013.1.1-1 Serious organised economic crime	CP-IP
	Topic SEC-2013.1.1-2 “Stronger Identity for EU citizens”	CP-FP
Area: 10.1.2 Intelligence against terrorism	none	none
Area: 10.1.3 Explosives	Topic SEC-2013.1.3-1 Inhibiting the use of explosives precursors	CP-FP
Area: 10.1.4 Ordinary crime and forensics	Topic SEC-2013.1.4-1 Smart and protective clothing for law enforcement and first responders	CP-FP
	Topic SEC-2013.1.4-2 Development of a Common European Framework for the application of new technologies in the collection and use of evidence	CSA (Supporting Action)
Area: 10.1.5 CBRN protection	Topic SEC-2013.1.5-1 European toolbox, focusing on procedures, practices and guidelines for CBRN forensic aspects	CP-FP
Area: 10.1.6 Information gathering	Topic SEC-2013.1.6-1 Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes	CP-IP
	Topic SEC-2013.1.6-2 Novel technologies and management solutions for protection of crowds	CP-IP
	Topic SEC-2013-1.6-3 Surveillance of wide zones: from detection to alert	CP-IP
	Topic SEC-2013-1.6-4 Information Exploitation	CP-IP
Activity: 10.2 Security of infrastructures and utilities		
Area: 10.2.1 Design, planning of buildings and urban areas	Topic SEC-2013.2.1-1 Evidence based and integral security concepts for government asset protection	CP-FP
	Topic SEC-2013.2.1-2 Impact of extreme weather on critical infrastructure	CP-FP
Area: 10.2.2 Energy, transport, communication grids	Topic SEC-2013.2.2-1 A research agenda for security issues on land transport	CSA (Coordinating Action)

	Topic SEC-2013.2.2-2 Toolbox for pandemics or highly dangerous pathogens in transport hubs – Capability Project	CP-FP
	Topic SEC-2013.2.2-3 Protection of smart energy grids against cyber attacks	CP-FP
	Topic SEC-2013.2.2-4 Cost effectiveness of security measures applied to renewable/distributed energy production and distribution	CP-FP
	Topic SEC-2013.2.2-5 Security of ground based infrastructure and assets operating space systems	CP-FP
Area: 10.2.3 Surveillance	none	none
Area: 10.2.4 Supply chain	Topic SEC-2013.2.4-1 Phase II demonstration programme on logistics and supply chain security	CP-IP
	Topic SEC-2013.2.4-2 Non-military protection measures for merchant shipping against piracy	CP-FP or Coordination and Support Action (Coordinating Action)
Area: 10.2.5 Cyber crime	Topic SEC-2013.2.5-1 Developing a Cyber crime and cyber terrorism research agenda	CSA (Coordinating Action)
	Topic SEC-2013.2.5-2 Understanding the economic impacts of Cyber crime in non-ICT sectors across jurisdictions	CP-FP
	Topic SEC-2013.2.5-3 Pan European detection and management of incidents/attacks on critical infrastructures in sectors other than the ICT sector (i.e. energy, transport, finance, etc)	CP-IP
	Topic SEC-2013.2.5-4 Protection systems for utility networks	CP-FP
Activity: 10.3 Intelligent surveillance and border security		
Area: 10.3.1 Sea borders	none	none
Area: 10.3.2 Land borders	Topic SEC-2013.3.2-1 Pre-Operational Validation (POV) on land borders	CP-CSA
	Topic SEC-2013.3.2-2 Sensor technology for under foliage detection	CP-IP
	Topic SEC-2013.3.2-3 Mobile equipment at the land border crossing points	CP-FP
Area: 10.3.3 Air borders	none	none

Area: 10.3.4 Border checks	Topic SEC-2013.3.4-1 Border checkpoints - hidden human detection	CP-FP
	Topic SEC-2013.3.4-2 Extended border security - passport breeder document security	CSA (Supporting Action)
	Topic SEC-2013.3.4-3 Security checks versus risk at borders	CP-FP
Area: 10.3.5 Intelligent border surveillance	none	none
Activity: 10.4 Restoring security and safety in case of crisis		
Area: 10.4.1 Preparedness, prevention, mitigation and planning	Topic SEC-2013.4.1-1 Phase II demonstration programme on aftermath crisis management	CP-IP
	Topic SEC-2013.4.1-2 Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and other unfortunate consequences	CP-FP
	Topic SEC-2013.4.1-3 Development of simulation models and tools for optimising the pre-deployment and deployment of resources and the supply chain in external emergency situations	CP-FP
	Topic SEC-2013.4.1-4 Development of decision support tools for improving preparedness and response of Health Services involved in emergency situations	CP-FP
	Topic SEC-2013.4.1-5 Preparing societies to cope with large scale and/or cross border crisis and disasters	CSA (Supporting Action)
	Topic SEC-2013.4.1-6 Preparedness for and management of large scale forest fires	CP-IP
Area: 10.4.2 Response	Topic SEC-2013.4.2-1 Fast rescue of disaster surviving victims: Simulation of and situation awareness during structural collapses including detection of survivors and survival spaces	CP-IP
Area: 10.4.3 Recovery	Topic SEC-2013.4.3-1 Shaping immediate relief action in line with the goals of development co-operation in post crisis / post conflict societies to maintain stability	CP-FP
Area: 10.4.4 CBRN response	Topic SEC-2013.4.4-1 Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination	CP-IP
Activity: 10.5 Security systems integration, interconnectivity and interoperability		

Area: 10.5.1 Information management	Topic SEC-2013.5.1-1 Analysis and identification of security systems and data set used by first responders and police authorities	CP-FP
	Topic SEC-2013.5.1-2 Audio and voice analysis, speaker identification for security applications	CP-IP
Area: 10.5.2 Secure communications	none	none
Area: 10.5.3 Interoperability	Topic SEC-2013.5.3-1 Definition of interoperability specifications for information and meta-data exchange amongst sensors and control systems	CP-FP
	Topic SEC-2013.5.3-2 Testing the interoperability of maritime surveillance systems	CP-CSA
Area: 10.5.4 Standardisation	Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products	CP-FP
Activity: 10.6 Security and society		
Area: 10.6.1 Citizens, media and security	Topic SEC-2013.6.1-1 The impact of social media in emergencies	CP-FP
	Topic SEC-2013.6.1-2 Varying forms of terrorism	CP-FP
	Topic SEC-2013.6.1-3 Trafficking in Human Beings: analysis of criminal networks for more effective counter-trafficking	CSA (Supporting Action)
Area: 10.6.2 Organisational requirements for interoperability of public users	Topic SEC-2013.6.2-1 Facilitators for assistance among EU Member States in emergencies in the EU	CP-FP or CSA (Coordinating Action)
Area: 10.6.3 Foresight, scenarios and security as evolving concept	Topic SEC-2013.6.3-1 Horizon scanning and foresight for security research and innovation	CSA (Coordinating Action)
	Topic SEC-2013.6.3-2 The evolving concept of security	CSA (Coordinating Action)
Area: 10.6.4 Security economics	none	none
Area: 10.6.5 Ethics and justice	Topic SEC-2013.6.5-1 Synthesis of results and reviewing of ethics, legal and justice activities in Security research in FP7	CSA (Coordinating Action)
Activity: 10.7 Security Research coordination and structuring		
Area: 10.7.1 ERA-net	none	none

Area: 10.7.2 Small and Medium Enterprises	Topic SEC-2013.7.2-1 Open topic for Small and Medium Enterprises: “Solutions for frequent petty crimes that are of high impact to local communities and citizens"	CP-FP
Area: 10.7.3 Studies	Topic SEC-2013.7.3-1 Increasing the engagement of civil society in security research	CSA (Supporting Action)
Area: 10.7.4 Other coordination	Topic SEC-2013.7.4-1 Trans-national cooperation among public security research stakeholders	CSA (Coordinating Action)
Area: 10.7.5 End-users	none	none
Area: 10.7.6 Training	Topic SEC-2013.7.6-1 Open topic for Small and Medium Enterprises: “Use of serious gaming in order to improve intelligence analysis by law enforcement agents”	CP-FP

- **Eligibility conditions**:

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

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

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

  - Proposals containing any classified information shall be ineligible.

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

- **Evaluation criteria for evaluating POV proposals**

  1. Scientific and/or technological excellence

     - Progress beyond the state-of-the-art.
     - Quality and effectiveness of the S/T methodology and associated strategy and work plan.

  2. Quality and efficiency of the implementation and the management

     - Quality of the consortium as a whole (including complementarity, balance).
     - Commitment of participating authorities.
     - Appropriateness of the allocation and justification of the resources to be committed (staff, equipment,…).

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

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

- **Evaluation procedure**:
  - The evaluation criteria and scoring scheme are set out in annex 2 of the work programme.
  - Proposal page limits: Applicants must ensure that proposals conform to the page limits and layout given in the Guide for Applicants, and in the proposal part B template available through the electronic Submission Services of the Commission .

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

    The minimum font size allowed is 11 points. The page size is A4, and all margins (top, bottom, left, right) should be at least 15 mm (not including any footers or headers).
  - A one-stage submission and evaluation procedure will be used.
  - Experts will carry out the individual evaluation of proposals remotely.
  - The procedure for prioritising proposals with equal scores is described in annex 2 of the work programme.

- **Particular requirement for participation, evaluation and implementation:**

Classified Information
Proposals must not contain any *classified information* (note that the proposed action itself *can* involve classified information). If classified inputs are required to carry out a proposed action or the output of the action needs to be classified, proposers have to ensure the following:
- provide evidence of the clearance of all relevant facilities;
- clarify issues such as e.g. access to classified information or export or transfer control with the National Security Authorities (NSA) of their Member States / Associated Countries, and provide evidence of the prior agreement of their NSAs;
- provide a Security Aspect Letter (SAL), indicating the levels of classification required at deliverables/partners level.

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

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

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

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

Small and Medium Enterprises (SME) and end-users
Consortia are strongly encouraged to actively involve *SMEs and end-users*.

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

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

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

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

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

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

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

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

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

IV. OTHER ACTIONS[58] (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[59] [60]: Electronic tools allowing the secured exchange of EU RESTREINT classified information**

  This action will be launched in the third trimester of 2013. Due to the possibility of managing classified reports in the context of a given project, there is a need for tools that could allow exchange of EU RESTREINT information via standard e-mail tools. The European Commission is willing to support the EU accreditation process of such a tool, which could be an existing one or a newly developed for this particular use. Open source solutions are welcome.

  Indicative Budget: up to EUR 1 000 000.[61]

  Funding scheme: Coordination and Support Action - public procurement

  Expected Impact: Facilitate the management of EU RESTREINT research projects

- **Call for tender[62] [63]: Development of statistical data on the European Security and Technological Industrial Base**

  This action in the second semester of 2013 aims at developing statistical data that would allow to obtain a clearer picture of the technological industrial base of the security industry in Europe. This would allow to obtain a better understanding of the strengths and weaknesses of the European security industry, as well as to better monitor the impact of R&D activities on the European security industry.

  As of today no reliable statistical data exists on the European security industry. The security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcom, etc.). The production of security-related items is hidden under a wide range of industry and services headings. Statistics for these headings do not distinguish between security and non-security related activities.

  Indicative Budget: up to EUR 750 000.[64]

  Funding scheme: Coordination and Support Action - public procurement

[58] 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).
[59] Call for tender can also be attributed via a framework contract.
[60] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.
[61] Under the condition that the draft budget for 2013 is adopted without modification by the budgetary authority.
[62] Call for tender can also be attributed via a framework contract.
[63] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.
[64] 'Under the condition that the draft budget for 2013 is adopted without modification by the budgetary authority.

Expected impact: A first compilation of statistical data on the European security industry

- 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 2 100 000.[65]

  Funding scheme: Coordination and Support Action – expert appointment letters

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

  a) Organisation of an annual Security Research event. Four service contracts are planned to be concluded in the second semester of 2013, and existing Framework Contracts will be used for this purpose.

  Indicative Budget: up to EUR 1 000 000.[66]

  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, to support an expert group on societal issues, to prepare information and communication material etc.

  Indicative Budget: up to EUR 900 000.[67]

  Funding scheme: Coordination and Support Action - public procurement, expert contracts

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

V. BUDGET

Theme SECURITY - Indicative budget

Activities	**2013[68] Budget EUR million[69]**
Call FP7-SEC-2013-1	299.33
General activities (cf Annex 4) (details below)	2,54
Other actions: • Evaluations (EUR 1.600 million) • Monitoring and reviews (EUR 0.500 million) • Actions implemented through public procurements and expert groups (EUR 3.650 million)	5.75
Estimated total budget	**307.62**

General activities - indicative budget

Activities	**2013[70] Budget EUR million**
CORDIS	0. 397
Experts (Evaluation and reviewers)	0.005
EUREKA	0.020
COST	2.115
Total	2,537

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:

- 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.

[68] Under the condition that the draft budget for 2013 is adopted without modifications by the budget authority.
[69] The Budget figures given in this table are rounded to two decimals points.
[70] Under the condition that the draft budget for 2013 is adopted without modifications by the budget authority.

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.