WORK PROGRAMME 2010

COOPERATION

THEME 10

SECURITY

(European Commission C(2009) 5893 of 29 July 2009)

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 justice, freedom and security[2], and to policy areas such as transport[3], health[4], civil protection[5], energy[6] and environment[7]. Through this, the Security theme also contributes to growth and employment in general, innovation and the competitiveness of European industry.

The respect of privacy and civil liberties is a guiding principle throughout the theme.

The Security theme has an exclusively civil application focus.

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

Following the recommendations of the Commission's *European Security Research Advisory Board (ESRAB)*[8], the Security theme addresses four security **missions** of high political relevance which relate to specific security **threats**. It contributes to building up the necessary **capabilities** – ESRAB identified 120 capabilities – for safeguarding security in these mission areas by funding the research that will deliver the required **technologies and knowledge** to build up these capabilities.

[1] http://ec.europa.eu/comm/external_relations/reform/intro/ip04_1151.htm; http://ec.europa.eu/comm/external_relations/cfsp/intro/index.htm;

[2] http://ec.europa.eu/justice_home/fsj/intro/fsj_intro_en.htm;

[3] http://ec.europa.eu/dgs/energy_transport/security/index_en.htm;

[4] http://ec.europa.eu/health/ph_threats/com/preparedness/preparedness_en.htm;

[5] http://ec.europa.eu/environment/civil/index.htm;

[6] http://ec.europa.eu/dgs/energy_transport/security/index_en.htm;

[7] http://ec.europa.eu/dgs/environment/index_en.htm;

[8] *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.*

It is clear however, 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 domains of **cross-cutting** interest are selected as well.

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

Security missions:

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 missions:

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

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

Technology oriented 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'** aim at building up and/or strengthening security capabilities required in the four security missions. This will be done through *adaptation of available technology* as well as the development of *security specific technology and knowledge aiming at tangible results.* In many cases these will also have cross-mission relevance.
  Average duration: 2-4 years
  Funding scheme: Collaborative Projects

- On the medium level of the building block structure, '**integration projects'** aim at mission specific combination of individual capabilities providing a security *system* and demonstrating its performance. They depend upon technology and knowledge building blocks carried out within capability projects or elsewhere.
  Average duration: 4 years
  Funding scheme: Collaborative Projects

- On the top level of the building block structure, **'demonstration programmes'** will carry out research aiming at large scale integration, validation and demonstration of new security systems of systems going significantly beyond the state of art. They depend upon the compatible, complementary and interoperable development of requisite system and technology building blocks of the integration projects and capability projects. They intend to promote the application of an innovative security solution, which implies a strong involvement of end users, taking into account the relevant legal and society related issues, and strong links to new standardisation. Demonstration programmes will be implemented in two phases:

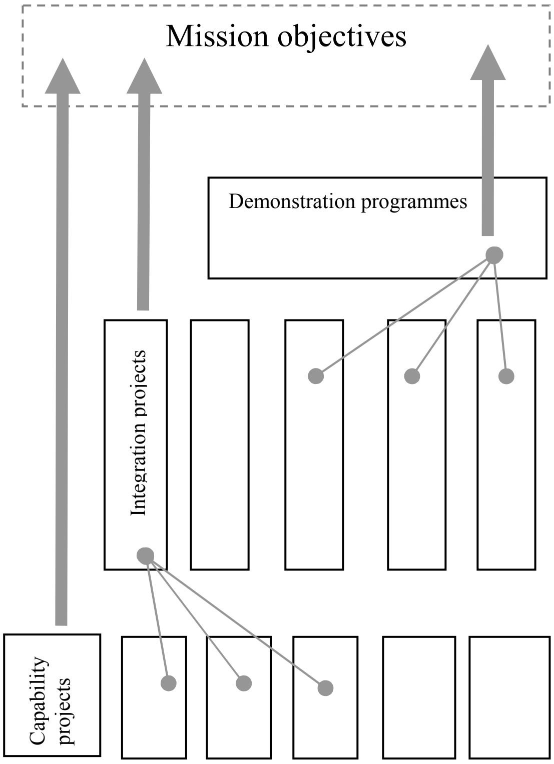

Figure 1: Research routes to meet the Security theme objectives

  <u>Phase I projects</u> (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.
  Duration: 1 – 1.5 years
  Funding scheme: Coordination and Support Actions

  <u>Phase II projects</u> (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.
  Duration (typical): up to 4 years
  Funding scheme: Collaborative Projects

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

The following funding schemes are envisaged:

The funding scheme **Collaborative Project** will, in the Security Research Call 3, be divided into *<u>capability projects</u>* (small and medium-scale projects, with indicative Community funding of EUR 3 500 000 and below), *<u>integration projects</u>* (large-scale integrating projects, with indicative Community funding of over EUR 3 500 000), and *demonstration programmes* (one or a number of individual projects) (large scale systems of systems demonstrations with an indicative funding of over EUR 20 000 000).

The **Networks of Excellence** scheme aims at research organisations that wish to combine and integrate in a durable way a large part of their activities and capacities in a given field, in a 'Joint Programme of Activities', possibly with a view of creating in this field a European 'virtual centre of research'.

For activity 6. *Security and society*, collaborative projects and coordination and support actions are possible as funding schemes (as appropriate). For activity 7. *Security Research coordination and structuring*, the funding schemes will be collaborative projects, networks of excellence and coordination and support actions (as appropriate). For the latter, 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.

Concerning the **Collaborative Project** funding scheme in the Security theme, the Community 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.[9] To claim this higher funding level, proposers need to demonstrate in their proposal that the required conditions apply[10]. Please note that demonstration activities are excluded from these provisions.

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

- **SME relevant research**

All actions are open to the participation of all security stakeholders: industry including SMEs (small and medium enterprises), research organisations, universities, as well as public authorities, non-governmental organisations and public and private organisations in the security domain. Considering the Security theme's objective of increasing the competitiveness of industry, the broad **involvement of SMEs** in consortia is highly encouraged.

- **International Cooperation**

All actions of the Security theme are open to **international co-operation** to industrialised countries as well as to ICPC[11] countries. At this stage, it is not foreseen to have any 'specific international co-operation actions' in the Security theme. These might be implemented at a later stage, in case participation of international partners through normal actions were deemed insufficient.

[9] *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*

[10] Claims for such higher funding level are in no way related to any of the evaluation criteria.

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

- **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. Suitable and dedicated coordination and support actions to achieve this could also receive funding. It is important to strengthen these activities in all projects.

- **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 consortia 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 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.

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

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

Due to the sensitivity of the Security theme, the *Rules for participation*[12] 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 3, **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 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

[12] *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*

provide a *security aspect letter*[13], indicating the levels of classification required. Appropriate arrangements 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 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.

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

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

The theme will also support **ERA-NET** activities (see more information in Annex 4), which are meant to develop the cooperation and coordination of research programmes carried out at national or regional level in the Member or Associated States through the networking of research programmes, towards their mutual opening and the development and implementation of joint activities. The Security Research Call 3 offers the possibility to submit a dedicated ERA-NET proposal under topic *SEC-2010.7.0-5 Co-ordination of national research programmes in the area of Security research.*

Research Executive Agency

Call for proposals under this work programme part (Security) will be implemented by the Research Executive Agency (REA) once this is operating autonomously according to the provisions of the Commission decision C/2008/3980 of 31 July 2008 “delegating powers to the Research Executive Agency with a view to performance of tasks linked to implementation of specific Community programmes People, Capacities and Cooperation in the field of research comprising, in particular, implementation appropriations entered in the Community budget”.

[13] ‘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.

The management of all projects to be funded as a result of this call for proposals will be implemented by REA, with the exception of:

- security sensitive grant agreements and contracts and
- policy related actions (indicated in section II of this work programme).

II CONTENT OF THE SECURITY RESEARCH CALL 3 (FP7-SEC-2010-1)

The primary ambition of the Security theme is to develop enhanced security related technologies, systems and systems of systems, and to facilitate their take-up for the implementation of security policies and programmes as soon as possible.

The main focus of the 2010 work programme will be on the 'demonstration programmes', which will be the 'flagships' of the Security theme as suggested by the ESRAB report. It includes Phase II demonstration projects in the two areas of: (i) European-wide integrated border control system, and (ii) security of mass transportation. Phase I of these two areas was already included in the 2007-2008 work programme. In addition Phase I of Aftermath crisis management is included in this work programme.

Furthermore, the Security Research Call 3 will include important topics that were not covered sufficiently well in the second Call FP7-SEC-2009-1, as well as 'capability projects' not covered earlier with a view to have a good basis of 'capability projects' on which 'integration projects' (IP) can be built upon in future calls. In parallel, and supporting this focus from the other building block levels, novel and improved technologies will also be developed, adapted and integrated into systems to be ready for the next generation of integrated security systems of systems to be demonstrated for full scale take-up in the future.

More attention has been given to the impact of the proposed technologies on the society, the organisational processes and the respect the human values which must be embedded in each proposal and foreseen in the work plan.

Also, a first step towards the definition of critical technologies for non-dependence and of new emerging technologies in the area of security is set out in order to define research priorities. This action should foster a European approach with a view to underpin/enable industry to acquire these technologies in the future.

The topics that are open to the submission of proposals under the Security Research Call 3 are described in the following sections.

Activity: 10.1 Increasing the Security of the Citizens

Area: 10.1.1 Demonstration programme

No demonstration projects are foreseen in this activity for the Security Research Call 3.

Area: 10.1.2 Integration projects

Topic SEC-2010.1.2-1 Information and knowledge management for the prevention of organised crime

Description of topic:
Current tools for the fight against organised crime include information technology systems, typically developed ad-hoc for each law enforcement agency, that are somehow capable to generate added value from disperse data sources by means of correlation, comparison and

tracking. The importance of these systems reside on their ability to provide evidence and warnings on facts that otherwise would not be detected during investigations and at the same time they can provide co-ordination between different agencies tackling same or similar actions or dealing with suspicious events/people.

However, considering the wide scope of potential parameters and variables to be taken into account, several limitations apply: dispersed sources of information; various formats (written, oral, digital, analogue…), language dependence; interoperability of systems; information sharing and security aspects of the systems and of the information itself; trans-national considerations; etc.

Through this action it is intended to tackle the availability of the widest range of information types and sources, data extraction and transformation tools and processes for knowledge management against organised crime. At the same time it should demonstrate the possibility of integrating them in a larger system, where each law enforcement agency is determined by its information offering and consuming capacities. Secure information handling is at the core of the system.

Then, the task, ideally driven by end-users (e.g. law enforcement agencies), is to show that a distributed system to be shared by the law enforcement agencies within EU, build by (re-) using systems and modules to be opened and integrated within an open architecture, can be effective to fight organised crime for the benefit of the EU. The systems and modules should be able to deal with information acquisition, processing and exploitation while taking into account legal issues within EU.

a) The issues related to **legal aspects** of the data to be collected/shared/exploited among different countries and agencies should be taken into account;
b) **Information acquisition** should use the means for all data-format (multilingual text and speech, video, image etc) and sources (open or closed source, disparate high volumes data repositories, network flows etc) to be collected and adequately stored and controlled;
c) **Information processing** should comprise all levels of data extraction, transformation, mining, etc;
d) **Information exploitation** should correlate real-time and historical data to allow automatic and under-demand (hypothesis building) analysis and decision-making, as well as support for the coordination of law enforcement actions through predictive/forecasting models to be used in prevention and mitigation actions.

Integration, interoperability, scalability and intrinsic security are to be key elements of this system.

Call: Security Research Call 3

Funding scheme: Collaborative Project

Expected Impact: *It is expected to 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; to demonstrate to the law enforcement agencies the added value to cooperate at the EU level while in the same time reducing their cost; to show to the EU citizens that this could be done without endangering individual liberties and privacy.*

Area: 10.1.3 Capability projects

Topic SEC-2010.1.3-1 Innovative tools to combat organised crime and terrorism financing and money laundering

Description of topic:
Disrupting, deterring and dismantling criminal financing networks is a key element of the fight against terrorist activities, as is detecting and preventing money laundering for the fight against organised crime. International standards and cooperation frameworks (such as Financial Action Task Force (FATF) and the United Nations) should be taken into account.

The objective is to develop innovative tools to help the detection and the prevention of money laundering and terrorist financing activities and more specifically to facilitate and improve its reporting mechanisms as well as the identification of money that has been stolen or robbed. European Strategy on Terrorist Financing sets banks and other financial institutions obligations of reporting suspicious financial activities to Financial Intelligence Units (FIU). Typical users of this tool would be private actors (e.g. banks), FIU and other public authorities or law enforcement bodies. The action will also include work on the legal framework at international, European and national levels, as well as the exchange of good practices within the stakeholders.

Call: Security Research Call 3

Funding schemes: Collaborative Project

Expected impact: *Taking duly into account the, mainly legal, context of Anti-Money Laundering and Anti-Terrorist financing, while involving the potential users, this action should provide an innovative and efficient tool to facilitate their activities. A significant improvement with respect to performance, reliability, speed and cost is expected. It will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation of the information, potential links to other related tools, privacy issues, international co-operation needs, communication strategies etc).*

Topic 2010.1.3-2 Tackling counterfeit medicines and related criminal networks

Description of topic:
Counterfeit medicines are a serious threat. The research activities will focus on identifying genuine medical products (including medicines, diagnostics and medical devices) by methods easily usable in the field as well as securing their legitimate supply chain. Important features are to identify and trace specific medical products such as research on fingerprinting of active pharmaceutical ingredients, tracing of individual tablets in a batch, innovative value added processes or technology focused solutions for individualising packs thereby ensuring product pedigree, etc. Additionally research activities may focus on how criminal organisations work. This could also include research on business networks for internet sales of counterfeit medical products.

Call: Security Research Call 3

Funding schemes: Collaborative Project

Expected impact: *The solutions proposed should offer the prospect of a significant reduction in the amount of counterfeit medicines and/or medical devices in circulation. The proposed innovative solutions must enhance and add value to existing EC initiatives.*

Topic SEC-2010.1.3-3 Detection of IED manufacturing facilities

Description of topic:
Improvised Explosive Devices (IEDs) are the explosive devices the most commonly used by terrorists and other criminals. They are considered as the most probable threat. Terrorist cells need a location to turn chemicals and/or explosives into IEDs: a "bomb factory". The objective of the topic is the development of capabilities to locate the bomb factory from tiniest of airborne, waterborne or contact traces using multiple sensitive sensors. The action should also investigate the innovative and efficient deployment of a network of sensors and the fusion of the information. The system should be able to minimise false positives. An in depth feasibility study as well as a detailed cost analysis of the envisaged system needs to be planned in the project but initial convincing elements have to presented in the proposal.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *Through an innovative and cost effective permanent monitoring of urban and sub-urban areas, the action would provide an early detection of suspicious activities and would alert counter terrorism units sufficiently in advance to prevent terrorist events.*

Area 10.1.4 Coordination and Support Actions

Topic SEC-2010.1.4-1 Advanced forensic toolbox

Description of topic:
The task is to develop best practises, methodologies and technological standards for the reconstruction of crime/terrorism scenes with the aim to improve interpretation and presentation in all stages of the legal process: from police briefings, case conferences through expert testimony in court without breaking the chain of custody. It should be applicable in all EU member states and associated states. This includes recommendations for the development of an open architecture and tools to support the proposed methodologies and standards for recording of crime scenes, scenario-driven evidence collection and decision making.

Call: Security Research Call 3

Funding schemes: Coordination and Support Action (coordinating action)

Expected impact: *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.*

Topic SEC-2010.1.4-2 Controlling the change of properties of chemicals to preclude misuse

Description of topic:
Publicly available chemicals have the potential to be used in terrorist scenarios. Chemical production, processing and consumption occur in tens of thousands of plant sites around the world each day. Chemicals are transported in various volumes and by various means of transport. Some of these chemicals have the potential to be used directly as, or precursors for terrorist attacks. An important first step to precluding their misuse would consist of (a) listing the potentially hazardous chemicals and their normal usage; (b) studying the possibilities of preventing their usage for terrorism without harming their normal function or safety properties; and (c) designing economically feasible methods of practically materialising some of the possibilities identified in stage (b).

Call: Security Research Call 3

Funding Scheme: Coordination and Support Action (coordinating action)

Expected impact: *This action should contribute to improve the traceability of property of chemicals that can be used in the preparation of terrorist actions, and therefore contribute to preclude such unwanted use.*

Activity: 10.2 Increasing the Security of infrastructures and utilities

Area: 10.2.1 Demonstration programme (DP) (either one or a number of individual projects)

Topic SEC-2010.2.1-1 Security of mass transportation - phase II[14]

Description of topic:
The objective is to create a 'system of systems' demonstration for security of mass transportation. A holistic and systematic all risks approach to assess, prevent, detect, prepare for and manage the threats to mass transportation / urban and regional transport security is being sought. Furthermore, the project should also aid the standardisation of solutions, to allow the creation of a European common market for future mass transport security solutions.

Focusing on the security of "Urban public transportation"[15]

The term 'security of mass transportation' covers both the security of transport infrastructures and services as well as the security of the passengers using transport services. The objective of mass transportation security in this demonstration programme is focused towards urban and regional public transportation. Accordingly, it includes: metro, tram, short distance regional rail transport (e.g. RER-Paris and the S-Bahn city busses, water buses, airport shuttles etc) while giving due consideration to the aspects of inter-modality, and other modes of transport. Key aspects of these systems are the very high numbers of passengers served on a daily basis and the fact that they are "open" with many points of access, which makes them hard to protect. Incidents at critical "neuralgic" nodes (such as transport interchanges, where long-distance and international transport is interconnected with urban transport systems) in dense

[14] Policy related action: the management of the grant agreement(s) will *not* be externalised to the REA.
[15] Further guidelines and relevant policy background in the area of Security, may be available from the dedicated Security Research web-site on EUROPA (http://ec.europa.eu/enterprise/security/index_en.htm).

and complex multi-modal network can have devastating effects, both in terms of casualties and disruptive effects on transport services, and should therefore be given special consideration.

Important infrastructures relevant to mass transport system should be considered in the project, such as: inner city stations, including their inter-functional spaces, tunnels, bridges, IT and communication systems and control centres (i.e. also protection against cyber-attack to these).

Freight transport is excluded from the demonstration programme, except for considerations of the risk-inducing role that transport of dangerous goods may have as a threat against passenger transport.

Appropriateness of security measures with respect to given legal, cultural and societal environment

The results of the demonstrator should be implementable, technically and economically, by providers and users/demanders e.g. the operators of urban public transport. Accordingly, a very strong participation from the 'demand side' is considered necessary; the security requirements capture need to rely heavily on those that are closest to the daily operations. The participation from the technology supply side (including the industry) is required to ensure that ambitious, yet realistic solutions are being pursued.

The right balance must be assured, thereby benchmarking, verification and validation of proposed solutions must be made by: operators and owners of mass transportation infrastructure (public and private), operator / franchiser / tenants in public spaces (restaurants, shops, booths, etc), intelligence services, security services (including private security companies), police, rescue services like fire brigades, urban transportation planners, civil society / human-right / privacy organisations, owner of real estate (stations, etc), manufacturers of mean of mass transport (metro rolling stock, busses, signalling system, communication system etc), passenger interest groups etc.

A testing phase in at least 3 real cities which area different from cultural background and urban public transport systems point of view should be foreseen.

The demonstrator should have a 'cohesion' effect, bringing several European cities and mass transport systems to participate in the project and by that share their experiences and best practices so as to broaden the basis of the project. This would be for the benefit of stakeholder organization and coordination, incident management, procedures, risk assessments etc.

Identification of the priority scope

Only through a holistic understanding of the security requirements of mass transport systems, will it be possible to define where security improvements are needed. In other words the stakeholders must be brought together, a risk-assessment and resilience analysis must be developed, and a cost effective security plan must be developed. Against this, off-the-shelf availability will be mapped and shortcomings identified.
Areas to be covered are e.g.:

- Security systems designed to meet specific requirements for mass transportation networks, transfer nodes and platform interiors;

- Interoperability of different security systems managed by different operators and/or between different EU countries;
- Comprehensive threat detection systems, fusing data across diverse and distributed networks and analysing threats via spatial/pattern recognition techniques. Detecting, tracking and tracing individuals, crowds and objects within, and across, transport systems, while respecting the personal integrity of individuals;
- Exploring ways of interconnecting urban transport data systems based on electronic ticketing/payment (for example: Oyster Card – London, MOBIB – Brussels, NAVIGO – Paris, and other similar) with other security systems;
- Preparedness and design for resilience, as well as post-event situation analysis systems capable of rapidly accessing and piecing together different multimedia and digital data to re-enact a sequence of events;
- Common operational picture, integrating and displaying data from a diverse set of sources on optimised man machine interfaces, handling the interagency aspects of mass transport security and utilising intelligence-based risk assessment and alert systems ;
- Neutralisation and containment systems for attack avoidance, suppression or nullification.
- Optimized interactions with the passengers, with regard to the newest consumer IT technology.
- Intervention and operations technologies wherever appropriate to cover synergies of security and safety and cost-effectiveness.
- Improving the protection, hardening and resilience of existing and new infrastructures related to mass transportation.
- New tools (e.g. simulation, virtual and augmented reality) to improve the training of the staff.
- Recommendations for operation procedures in case of a security situation.

The interoperability requirements will drive standardisation in this area. Accordingly interoperability should also be seen as a means to create the European wide market for equipment for these applications.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *The DP should provide a demonstration of "system of systems" solutions to enhance the security of urban public transportation for typical big and mid-sized European cities with over 0.5 million inhabitants. The challenge, the demonstrator has to tackle, is the security of mass transport in a metropolitan area and the proposed solution should be benchmarked according to their impact on improved security. The systems / technologies demonstrated should be demonstrated with 'real hardware' in a number of relevant places in addition to any modelling and simulation.*

The DP would nonetheless be required to have a fully European dimension, and make best use of the pertinent projects conducted within the national and /or European frameworks, focusing on their possible integration with a view to better responding to meeting operational challenges. The DP should make it possible to bring together private and public end users from many countries, able to provide the input data of the pertinent scenarios as well as the assessment (validation/test) criteria.

Area: 10.2.2 Integration projects

No integration projects are foreseen in this activity for the Security Research Call 3.

Area: 10.2.3 Capability projects

Topic SEC-2010.2.3-1 Planning, (re)design, and (re)engineering of urban areas to make them less vulnerable and more resilient to security threats

Description of topic:
Based on risk assessment and modelling, the first task is to develop a framework to be able to identify in existing urban area (including public spaces such as public transport terminals, sport venues, shopping and business centres) 'weak points' where security must be reinforced. The second task is to define/develop tools to be able to develop more robust and resilient 'space' in the field of urban planning/design/engineering. The resulting urban space itself should be such that it is less prone for and less affected by attacks/accidents including natural disasters. All auxiliary infrastructures supporting such an urban space should be covered in the proposal. A primary goal should be to protect the human beings and the surrounding natural environment. In both cases, comprehensive supporting tools must be developed in a sufficient generic status such that applications to different type of urban environment (also in old and new cities) could be easily done. Concepts for the assessment of existing security cultures and their development, training concepts, acceptance analysis have to be included as part of the project.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *It is expected that action under this topic will improve the design of urban area and thus increase their security against and resilience to new threats. It will also contribute towards the protection of human lives and environment.*

Topic SEC-2010.2.3-2 Assessment framework and tools to identify vulnerabilities of energy grids and energy plants, and to protect them against cascading effects

Description of topic:
The task is 1) to develop risk assessment tools to identify vulnerabilities in energy distribution grids and energy production, plants, 2) to develop tools to protect these critical infrastructures against cascading effects and against deliberate acts of terrorism and sabotage etc. and 3) to carry out contingency analysis of the distribution networks/grids and to plan automatic restoration and intelligent reconfiguration in case of failure of parts of the network. Energy production plants and distribution sites are very sensitive and if they are destroyed damaged or disrupted it can have significant, cascading, impact on the surroundings (environmental, economical etc) and the overall functioning of the society (security of supply etc). These sites can be targets of deliberate acts of terrorism, sabotage, criminal activity, malicious behaviour etc or they can simply be affected by accidents, natural disasters, negligence and so on. Firstly, priority is on reinforcing the energy grids and plans against above threats and secondly on evaluating the potential impact of a failure and the steps that need to be taken to

re-establish the overall energy system. Work that has already been undertaken at EU and international fora should be taken into account.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *It is expected that action under this topic will provide significant improvement in the security and resilience of complex interconnected energy networks. Actions will analyse the vulnerabilities of the different parts of the network and provide tools to limit the impact of accidents/attacks etc on these networks.*

Topic SEC-2010.2.3-3 Automatic detection and recognition of threats to critical assets in large unpredictable environment

Description of topic:
The task consists (1) to develop tools that integrate smart surveillance information system and (2) to improve relevant sensors in terms of affordability, autonomy, robustness and display from heterogeneous critical assets (e.g. mobile assets and/or temporary sites/plants). These assets may possibly be loosely or not at all connected to Internet and located in large area without protection and/or in harsh/hostile environment. In order to build up high level local situation awareness, the task is also to develop signal and information technologies especially for automatic sensor processing and data fusion for this type of environment, presentation techniques and methodologies for validating and certifying the detection system efficiency. Field trials should be foreseen in order to test different scenarios related to needs. The objective is to enable optimised protection decision making required for protecting these particular types of assets.

Call: Security Research Call 3

Funding schemes: Collaborative Project

Expected impact: *An integrated, scalable, affordable and easy to deploy detection system meeting requirements for a broad range of scenarios and missions related to the critical assets and aiming to establish a European reference and set of tools for efficiency evaluation of detection and monitoring system, leading in the long-term to European standards*.

Area 10.2.4 Coordination and Support Actions

Topic 10.2.4-1 New concepts to meet the requirements for the protection of civil/commercial aviation

Description of topic:
With the continuous development and proliferation of technology, new opportunities on the one hand, and risks on the other, in relation to the security of aviation, have to be faced in the near future. Within this action, the expectation for the future of these emerging opportunities and risks should be explored, and concepts to mitigate threats and to make use of emerging opportunities should be identified, taking into account European/international ongoing and planned activities for protecting the civil/commercial aviation. The state of relevant European

capabilities should be catalogued and compared against relevant requirements, and a counter-measure/opportunity roadmap should be recommended, taking also into account cost aspects. This includes:

- A comprehensive view on new technologies and proliferation issues, and their impact on the protection of civil/commercial air transportation (including airports) against attacks (e.g. MANPAD, EMP, microwave-weapons, virtual radar etc).
- The definition of potential risks and future challenges in the area of civil/commercial aviation, taking into account all possible solutions to mitigate the threats and to make use of emerging opportunities (ground and onboard; air-side and land-side; day-to-day operation; natural, man-made disasters and terrorism; short term, medium term and long term etc).
- The management of standardisation issues (such as threats, aircraft, airport, efficiency of solutions), export control and non-dissemination, certification (safety aspects), environmental constraints, operational and costs aspects.
- European technical recommendations and tools to enable future regulation for example exploring new possibilities offered by interconnection of security database and airline database, which maybe be supported by biometric technologies.
- A cost-benefit analysis of the implementation of the different security scenarios, including operational and maintenance constraints and requirements for the airliners.

Proposers can choose: (i) to assess the whole spectrum of possible threats/opportunities to civil/commercial aviation and/or (ii) to focus on specific forms of threats/opportunities (e.g. MANPAD).

Call: Security Research Call 3

Funding schemes: Coordination and Support Action (both coordinating and supporting action)

Expected impact: *To build a comprehensive European approach to counter possible threats and to make use of emerging opportunities in the area of civil/commercial air transportation and airport (e.g. attacks by MANPAD) within a consortium including a wide range of stakeholders (airports authorities, commercial aviation users, Governments and European bodies and industry). The added value of the action at European level will be to improve the European ability to counter possible threats and future challenges and to initiate the building of a solid European position through the definition of a "European approach to secure civil aviation".*

Activity: 10.3 Intelligent surveillance and enhancing border security

Area: 10.3.1 Demonstration programme (DP) (either one or a number of individual projects)

Topic SEC-2010.3.1-1 European-wide integrated maritime border control system - phase II[16]

Description of topic:

[16] Policy related action: the management of the grant agreement(s) will *not* be externalised to the REA.

The objective is to address one of the most challenging problems faced at the EU external borders, namely to improve the capability of Member States' authorities to detect, identify, track and intercept vessels, including small fast boats, used for illegal migration and related cross-border crime.
Information sharing is the key element to improve the situational awareness at the external maritime borders, thus requiring the development of a common information sharing environment, in which data from different sources and security domains will be discoverable, accessible, understandable, fused, and usable, with appropriate information assurance, to enable common situational pictures.

The demonstration programme will therefore cover only the maritime portion of the EU external borders. Maritime border surveillance is intrinsically complex. Europe has about 90 000 km of coastline along two oceans and four seas. Maritime surveillance requires end-to-end continuity from ports, coastlines and territorial waters to high seas as well as, if appropriate, neighbouring third countries. Mandatory information obtained from ships is to be complemented by additional external information, i.e. for the monitoring of small boats and of non-cooperative vessels as well as and, where appropriate, information from maritime ports and extended border zones.

No single technological solution exists capable to meet the variety of operational requirements. Additional elements add complexity at the integration level, for instance:

- the legal aspects of information exchange (provided by systems historically developed for different purposes),
- the acquisition and exchange of information on a 24/7 basis,
- the sharing and fusion of information to obtain a common situational picture,
- the regulations for priorities for delivery (or denial) of access.

Currently, information systems existing in the various national organisations are structured in different ways; often they are not interoperable, and data is not always made available to others. The primary issues are of organisational and political rather than technological nature. However a degree of convergence can be anticipated to progressively take place during the time of implementation of this DP (completion estimated not earlier than end of 2014).

A key aspect of the implementation of the EU Integrated Border Management is the development of a European Border Surveillance System (EUROSUR)[17]. This proposed DP, although it is an initiative of technological nature, is considered to potentially pave the way towards a more pro-active approach in the future EUROSUR cooperation mechanisms.

In this context, the national authorities responsible for maritime border surveillance and FRONTEX are expected to be the main ***end-users*** of this DP. Typically, a wide variety of national authorities are involved in the control of the maritime borders and of the ports; different authorities having responsibilities for surveillance, overall security and migration control of the contiguous zones, the territorial waters and the coastlines and the ports; sometimes with parallel competencies, but with different reporting lines. Border police and Customs are important national authorities, while EMSA is a relevant EU Agency.

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

The EU has recently introduced Joint Maritime Operations coordinated by FRONTEX involving various services (Navies, Coastguards, Customs, Border Police, etc.) and assets (patrol boats, frigates, helicopters, aircraft, etc.) with limited interoperability (modus operandi, procedures, language, communications assets). Further development of joint operations calls for interoperability and standards, operational as well as technical, between the different units. This concerns many technical systems, including communications and geographical information systems.

For the 2015 time horizon, innovative solutions should be set up to permanently monitor and track all type of ship traffics, vulnerable trading lanes, maritime ports and extended border zones, and to detect abnormal behaviour to understand and identify risks and threats at an early stage and to respond as appropriate in full respect of human rights and in particular the rights of asylum seekers.

This future generation of maritime surveillance capabilities should allow:

- Permanent and all weather coverage of maritime areas;
- Continuous collection and fusion of heterogeneous data provided by various types of sensors and other intelligent information from external information sources;
- Supervised automatic detection of abnormal vessel behaviours (tracks and activities) and to generate documented alarms;
- Understanding of suspicious events and early identification of risks and threats from series of detected spatiotemporal abnormal vessel behaviours (alarms);
- Detection and tracking of scrapping vessels used for illegal migration;
- Detecting and preventing illicit movements of persons and goods through multi-layered and end-to-end surveillance.

No equipment and information system in operation or under deployment is currently able to answer all the above requirements. However, by the 2015 time horizon significant technical progress is expected with respect to wide maritime area coverage, combining different sets of sensors and platforms, heterogeneous data processing and fusion, using new methodologies for detecting abnormal behaviours. These should be usefully integrated to build up an innovative maritime border surveillance system for national, regional and European missions to efficiently provide border security applications in remote as well as high density traffic areas. Development of different non-compatible systems should be avoided.

The most important challenges identified are the detection of small craft, fusion of information in order to detect anomalies, interoperability and affordability.

Detection of small craft: The main challenge is detecting, identifying and tracking small (possibly fast) craft in vast areas of open seas as well as in closed waters of archipelagos. Another challenge would be the detection of low flying aircraft. Different sensor solutions (including, if appropriate, patrolling assets and coastal surveillance capabilities) would need to be demonstrated and integrated to provide adequate performance.[18]

Fusion of information and establishment of a situational picture at regional and European level: Information coming from real time sensors needs to be integrated with intelligence

[18] It should be noted that development on space-based observation and assessment tools is undertaken in the WP for Theme 9 ‘Space’.

information coming from tracking ship movements and container movements, information coming from a pre-frontier intelligence picture and from human sources. This should serve to detect anomalies both at sea and land/sea interfaces and to assess different threat levels.

Presentation of the information: Measures to present the fused information in order to provide decision support to the operators would need to be demonstrated.

Interoperability: The demonstrated solutions need to provide interoperability between different organisations in different states. Furthermore, integration of some legacy systems will have to be demonstrated.

Information provided by existing space based capacities and services, as well as by relevant activities under the FP7 Space theme, should be taken into account where appropriate.

The DP should provide a demonstration of 'system of systems' solutions for border surveillance and control, in terms of extended situation awareness providing a fit for purpose situational picture, to be initially tested at a selected portion of the maritime external borders of the European Union.

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

This assessment should not be limited to only those active as partners in the project, as these alone may not be representative of all those concerned at EU level. For this reason a mechanism should be set up ensuring that, whatever the consortium retained, pertinent private and public end users ("first buyers") would be integrated to the assessment and the follow up of the work. This mechanism should bring together representatives of EU authorities (and agencies) and representative (both public and private) appointed by the Member States. This panel should be involved in the establishment of assessment and demonstration criteria in an operational context as soon as the project starts. Public end-users should also guide and monitor the possible handling of sensitive information.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *The DP should demonstrate key elements for a future common information sharing environment providing situational awareness of activities (in particular those unlawful) at external maritime borders with continuity from high sea, to coastal waters and ports, on the basis of sharing and pooling maritime surveillance assets (at MS and EU levels) and in full compliance with sovereign prerogatives and information ownership requirements.*

The research nature of the proposed DP implies restricting its perimeter to one or a number of demonstration exercises in a clearly identified place and time, specifying the target (or targets), the threats and the associated scenarios.

The DP would nonetheless be required to have a fully European dimension, and make best use, at the system of systems level providing continuity in surveillance from open seas to coastal waters and ports, of the pertinent projects conducted within the national, regional and/or European frameworks (e.g. other projects related to maritime and port security supported by FP7 aimed at improving the technical performance of sensors and at the fusion and analysis of information), focusing on their possible further integration with a view to better responding to meeting operational challenges. The DP should make it possible to bring together from many countries the private and public end-users able to provide the input data of the pertinent scenarios as well as the assessment (validation/test) criteria. Strong end user involvement, including whenever possible on the basis of other EU funded initiatives, would be particularly important to demonstrate how modern technology can facilitate the needed interagency cooperation inside and between States, via information sharing on a need to know basis in order to meet the challenges even under severe conditions.

Area: 10.3.2 Integration projects

Topic SEC-2010.3.2-1 Monitoring and tracking of shipping containers

Description of topic:
The aim of the research is to provide the technology and information gathering mechanisms contributing to the implementation of a system for the monitoring and tracking of EU (inbound and outbound) container traffic, possibly at the global scale, effectively identifying (and possibly coping with) security threats. Such traffic may come in on a variety of vectors (i.e. trucks - trains, barges and increasingly feeder vessels, but predominantly by intercontinental sea transport).

The system should be based on a sound risk based approach to container security, i.e. the system should be capable of identifying possible manipulations and all those containers that possibly pose a threat to security, which can then be further scrutinised. The system should combine different technologies, like container tracking and localization, tamper proof sealing, container-integrated sensor technologies, statistical methods and data available on the container to provide a holistic approach. Also concerns of data security and data transmission between authorities should be addressed. In this context the safeguarding and guaranteeing the information chain is a key issue.

For the development of such information gathering systems, business drivers and collateral benefits are important conditions for a broad acceptance by business parties. Furthermore, the research should focus on the required information set from the point of view of supervision agencies (such as customs, Interpol and veterinary inspection agencies), and the availability of that information in the supply chain. In addition, monitoring of in- and outbound container traffic will generate a requirement for protocols to handle exceptional traffic, and traffic that has been flagged as suspect, unsafe, or potentially dangerous. Finally, given that business has to accept and cooperate with initiatives to start monitoring their container traffic, there should be not only stability from a technical and organizational point of view but also a clear business model, with quantifiable benefits, and a cost-benefit analysis for the monitoring and tracking of the containers. It should also reduce the clearance time and possibly reduce the insurance premiums (i.e. an effective crisis management strategy would be set up in case something goes wrong).

Hence, in addition to the technical developments, the following activities should be addressed:

- definition of business drivers and collateral benefits;
- definition of the required information set by supervisory bodies;
- integration of this information in the supply chain management processes;
- definition of protocols to handle exceptional or suspect traffic;
- definition of a crisis management strategy when needed
- compliance with privacy and human rights issues and in particular the issues raised by asylum seekers.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *The system for the monitoring should allow for a permanent and reliable localization of containers, as well as differentiation of the content of containers, while guaranteeing and safeguarding the information chain and triggering necessary countermeasures.*

Area: 10.3.3 Capability projects

No capability projects are foreseen in this activity for the Security Research Call 3.

Activity: 10.4 Restoring security and safety in case of crisis

Area: 10.4.1 Demonstration programme (either one or a number of individual projects)

This Security Research Call calls for the first phase of this demonstration programme, which will define its strategic roadmap and ensure Europe wide awareness.

Topic SEC-2010.4.1-1 Aftermath crisis management - phase I

The scope and technical content of the full demonstration programme (phase II, which will build upon phase I) will be the demonstration of an integrated and scalable crisis management system capable of providing comprehensive situational awareness to decision makers to ensure a timely, co-ordinated and effective response to large scale disasters, including natural disasters (floods, earthquakes etc) both inside and outside Europe.

Large-scale incidents require a coordinated response from crisis managers and first responders from different agencies across Europe and with resources from all levels of government. A common operational picture, well trained and equipped teams, secure communications, and flexibility in planning/executing crisis management missions (man made and natural) are the underpinnings of crisis management.

Activities should cover some or all of the following areas:

- Interoperable secure communication systems
- Robust and scalable wide-range and persistent situational awareness systems that combine and integrate, in real time data from different systems to improve decision making.

- Network enabled capabilities and decision support for shared command and control that can be adapted to the availability of different parties that participate in the crisis management operations.
- Comprehensive logistic and resource planning systems to enable a rapid response, inside and outside Europe.
- Robust, lightweight and mobile search and rescue systems for all situations
- Portfolio of solutions for interagency/international training, exercises and best practice exchange based on realistic modelling and simulation tools.
- Development and adaptation of national and international operating procedures and organisational structures to a common or interoperable crisis management system.
- Rapid, relevant and dynamic post incident systems to restore basic services (energy, transport, telecoms)
- Methodology and tools for medical care,
- Fast deployment in harsh environment.

Scope of Phase I (open): The action will define the strategic roadmap required for the demonstration programme which should take into account relevant completed, ongoing and planned work and lay out, in a coherent and clear manner, the further research work required. It will assess the relevant factual and political situation and trends as well as potential classification requirements and issues related to IPR, also with a view to procurement. It will ensure EU wide dissemination of the preparation of the demonstration programme proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the cooperation of third country participants is required or recommended.

Call: Security Research Call 3

Funding scheme: Coordination and Support Action (supporting action)

Expected impact: *Through comprehensive preparation (not proposal preparation) of the demonstration programme, the action will provide a solid basis for the description of its phase II as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified Europe wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration programme identifying key players and performance profiles of other required contributors, allowing for their effective and balanced access to the action. It will also achieve qualified Europe wide awareness of relevant end users, governments and other bodies, facilitating and providing guidance concerning the real-life implementation of the system of systems to be demonstrated.*

Area: 10.4.2 Integration projects

Topic SEC-2010.4.2-1 Interoperability of data, systems, tools and equipment

Description of topic:
The task is to address the needs for improved systems, tools and equipment for "the command and control" function of emergency management organisations and their harmonisation at European level. The goal is to ensure an effective management of large civil crises and complex emergencies (either man-made or natural) by strengthening command and control capabilities throughout the phases of the crisis management process (prevention, preparedness, response and recovery, including simulation and training). Participating

organisations and nations commonly have different mandates, goals, means and methods of handling crisis, which makes cooperation difficult. Technology is a critical tool for improving interoperability, but it is not the sole driver of an optimal solution, as cooperation requires harmonised rules, procedures and processes. Successful implementation of data, systems, tools and equipment technology should be supported by strong leadership and is highly dependent on effective collaboration and training among participating actors and countries. Therefore, there is a need to create and demonstrate the development of new and integration of existing solutions into a common set of data, tools, systems and equipment that are interoperable in order to support: a) access to and distribution of relevant information (including different data formats, sources, data transformation etc); b) early warning and alert infrastructure; c) response planning and management, based on shared operational picture and situational awareness between first responders; d) coordinated asset localisation and management, during large emergencies across organisational and geographic boundaries. The proposed solution should be set up and tested in a real environment e.g. as a proof of concept. The expected outcome would be interoperable data, tools, systems and equipment that help crisis management structures in complex emergencies and crises across organisations and countries and cope with their heterogeneity.

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *Actions in this area will provide the adapted data, tools, systems and equipments technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and (private and/or public) end users. Significant improvements will be achieved with respect to performance, reliability, speed and cost. Actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. It will also cover important issues such as harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.*

Topic SEC-2010.4.2-2 Preparedness and Resilience to a CBRN crisis

Description of topic:
The perspective of a terrorist group using non conventional weapons such as CBRN (Chemical, Biological, Radiological and/or Nuclear agents) materials is commonly seen as more and more probable. The consequences of a terrorist CBRN event could be particularly dramatic regarding the number of casualties and/or the created panic. In case of an event, it could take some time (days or weeks) to identify it. An early detection could significantly reduce its impacts. In order to contain and limit the effects of such an event due to terrorists or linked to industrial accidents, the task is 1) to integrate capabilities and to develop a system of tools and methods to improve and coordinate operational reaction following the occurrence of the event 2) to develop information and training kits to the public and to specific audiences envisaged before (preparedness) and after the event (response). The system includes early warning systems, isolation, shielding, decontamination, medical counter-measures etc. Societal reaction, communication and human factors for first responders, political deciders and the public have to be considered. The action could include the handling of casualties in hospitals analysis and comparison of the different organisations set up to deal with casualties throughout Europe, exchange of good practices at the European level.

Call: Security Research Call 3

Funding scheme: Collaborative Project

Expected impact: *While taking duly into account the legal and political background, the action will lead to a complete toolbox to be used by public authorities in charge of crisis management (incl. health authorities). It should lead to an integrated European approach to CBRN crisis. It should provide and demonstrate significant improvements with the existing fragmented situation and significantly improve the resilience of the European Union.*

Topic SEC-2010.4.2-3 Information acquisition using dedicated platforms, including UAV, aerostatic platforms (balloons) and satellites[19]

Description of topic:
Situation awareness as required by governmental services in charge of the management of emergencies (also outside the EU), law enforcement, progressively relies on the effective real time monitoring and surveillance of wide areas. Substantial improvements in capabilities are expected to be obtained by combining, at the system level, information derived from a variety of different platforms (e.g. unmanned aerial systems (UAS) and aerostatic platforms (such as balloons)) possibly complementing, where appropriate, data provided by satellites. The technical requirements of the systems to be developed and their level of performance need to be analyzed, specified and tested, within properly identified scenarios, in terms of detection, identification, and monitoring capabilities of the items of interest for the targeted application. At the system level, emphasis should be put on communication requirements. In particular, communication specifications will have to be considered in terms of integration in the traffic and of capability to reinforce the effectiveness of the mission. The research work should be undertaken in close liaison with users (such as the Civil Protection and Law Enforcement organisations) and with regulators (e.g. Civil Aviation authorities). Activities should include the evaluation, over a range of crises management missions, of the possibilities being offered by the development of novel sensors specific for surveillance and security purposes, and by the novel integration of data that would be provided by versatile multi-functional equipment, also UAS borne (e.g. aerial and survey photography using IR, signal and spectral analysis and miniature synthetic aperture radar and related data exploitation). A particular challenge to be addressed is identified in the miniaturisation of components to make the system more versatile, performing and with a guaranteed quality of service

Call: Security Research Call 3

Funding Scheme: Collaborative Project

Expected impact: *Improved capabilities are expected for situation awareness as required for the effective management of emergencies and actions of law enforcement. They would be based on more effective real time monitoring and surveillance of wide areas. These capabilities, to be validated at the European level by official public users in realistic scenarios, are expected to demonstrate the potential for delivery of novel services, and the potential for their possible rapid take up by different Member States. The project is also expected to pave the way to the revision of regulations, at the European level, for them to be*

[19] It should be noted that development of space-based observation and assessment tools is undertaken in the WP for Theme 9 ‘Space’.

less limiting with respect to the use of surveillance systems in key areas of civilian importance.

Area: 10.4.3 Capability projects

Topic SEC-2010.4.3-1 Alert and communication, including the role of media, towards the population in crises management

Description of the topic:
The task is to develop innovative methodologies and technological solutions to manage alert and communication in crises management. This includes:

- Evaluation and re-assessment of alert procedures and processes in order to cope with new, complex and recurrent crises.
- Screening of the information structure (content, explaining…) between all kind of actors taking into account intercultural factors, communication toward the population and consistency with response and rescue of on-going operation, recurrent crisis communication management and the familiarisation of the public (false alert problematic).
- Analysis of the role of mass media (in particular new ones) during crises and the best practices in their use in order to ensure effective and ethical crisis management while respecting the freedom of the press.
- Technological solutions, e.g. agent-based simulation platforms, to perform what-if analyses of the efficiency of communication plans, to prevent communication pitfalls and support better information exchange between authorities, crisis management stakeholders and citizens

Call: Security Research Call 3

Funding schemes: Collaborative Project

Expected impact: *Efficient communication about possible or actual emergencies can be fundamental to prevent them. Contemporary alert, communication concepts, procedures and technological simulations for effective crisis management will improve the planning and the response during and after an incident.*

Topic SEC-2010.4.3-2 Adaptation of existing Decision Support Systems (DSS) to new radiological threats

Description of topic:
The existing decision support systems (DSS) for radiological emergency management are not able to deal with new radiological threats. Such incidents are often characterised by an unknown source term (nuclide composition, total activity), little information on the location of the source, time and duration of the release, area and number of people affected. Of particular importance is that there might be no warning phase. Potential scenarios are among others:

- stolen sources which are brought to a public place,
- contamination of important locations such as airports or underground stations with contaminants (spray attack)
- contaminated food and drinking water
- transport accidents

- radiological dispersal device

The assessment for these incidents can only be partly performed with existing DSS. Radiological Dispersal Device and transport accidents can be described with existing models but specific threats such as contamination of buildings or underground stations are out of their scope at present. The most critical aspect, however, is the ability to provide an assessment without knowing much about the contaminant and the close interaction with the commander in chief at the local level. This requires a complete modularisation and a more flexible handling of the existing DSS to be applicable for the new threats. Simple approaches have to be developed allowing to estimate the risk to the public without having a complete picture of the potential source term or contamination pattern. These models have to be so flexible but also simple that they can be readjusted by experts using them at the spot. The modularisation would allow to tailor the system to the needs of the various clients from a radiation protection centre in a country to the fire brigade command post responsible at the spot.

The action should cover:

- Development of modular, simple and flexible models for the assessment of the dose under high uncertainty
- Development of a data base supporting these models that they can be easily adapted and adjusted to different circumstances
- Development of a framework for these models to allow them to be applied at national centres together with existing DSS and locally in the command and control centres of the fire brigade/police
- Development of transport and dispersion models for large buildings such as airports and other large public buildings
- Development of transport and dispersion models for underground systems
- Development of interfaces with local Command and Control systems to use the models in strategic (DSS) and local systems

Call: Security Research Call 3

Funding scheme: Collaborative Project

Expected impact: *The action will contribute to a significant improvement in the capacities of the European / national / regional authorities in charge of radiation protection to handle new radiological threats.*

Area: 10.4.4 Coordination and support actions

Topic SEC-2010.4.4-1 Basic service restoration (e.g. energy, water, communication), business continuity, domestic/environmental normality

Description of topic:

The task is to study existing services (e.g. energy, water, communication), and then to provide different scenarios and approach that organisations and members states could adopt in case of large crisis. The ultimate goal is the business continuity and domestic/environmental normality. The project should present a number of realistic scenarios /solutions of basics "real" services restorations. The project should also take into account the border dimension in the scenarios/solutions presented (i.e. the possibility to re-use one or more of the border member state facility e.g. energy, water, communication).

Call: Security Research Call 3

Funding Scheme: Coordination and Support Action (coordinating action)

Expected impact: *While taking into account the border dimension of the EU member states and associated countries and human factors as well as related cross-border issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. Scenarios, solutions and standardisation issues will also be identified in order to fulfil the business continuity, domestic/environmental normality and also foresee further research needs with a view to future security research work programmes.*

Activity: 10.5 Improving security systems integration, interconnectivity and interoperability

This activity is not open for self-standing actions in the Security Research Call 3. However, proposals dealing with system integration, interconnectivity and interoperability issues related to the four missions can be submitted under activities 1,2,3 and 4 and will be considered ‘in scope’ there, as long as they are equally in line with the corresponding technical content and scope.

Activity: 10.6 Security and society

Security, whilst very important, is just one of the societal values in Europe which must be balanced against others. The EU Member States have all signed up to the European Convention on Human Rights and promoting the values of human dignity, freedom, democracy, equality, the rule of law and respect for human and minority rights. It is therefore required to respect these different values which will need to take account of variances between countries, circumstances and integrate them when addressing the development of threats and their perceptions.

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

Actions in this activity will provide improved insight and advice for security policy makers, security research programme makers and (mission oriented) security research performers (in some cases, acting as “Think Tanks”). They aim to obtain a broad and well-based understanding of the public administrative, cultural and societal frameworks in which security enhancing policy measures, including in particular security research, take place. In particular they effectuate in-depth understanding of the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. The outcome of the research together with appropriate dissemination strategies contribute to the effective and efficient planning and designing of future security research programmes and actions as well as to policies, programmes and initiatives which enhance the security of the European citizens.

As this activity takes a threat and incident related approach only, it is complementary to the more general approach of Theme 8 *Socio-Economic Sciences and the Humanities*, 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. Security is addressed as one of these challenges and set in the general landscape.

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

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

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

Area: 10.6.1 Citizens and security

The security of the European citizens is at the core of the Security theme. 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 in particular address violent radicalisation risks, terrorist behaviour and activity etc. Thus it will provide authorities as well as future technology related research with valuable information and recommendations to improve their performance.

Topic SEC-2010.6.1-1 Signs of 'early warning' to detect trends and weak signals in social polarisation, radicalisation development and segregation

Description of topic:
The task is to obtain a deeper understanding of the signs of 'early warning' and weak signals of social trends that may lead to violent extremism and even terrorism (e.g. polarisation, radicalisation development and segregation at collective or individual level), in order to facilitate effective policies and counter-measures and increase the society resilience. The first goal should be to use these signs to build indicators allowing to curb, to stop and to prevent these social processes. The second goal should be to understand whether and how specific contextual and structural conditions (e.g. residential segregation, social exclusion, unemployment etc) may foster the adoption of extremist views resulting in violence/terrorism. Thirdly, technical and social environment (including Internet) should also be considered because they create norms and boundaries as well as possibilities for terrorist activities. The internet should be treated as a stand alone context insofar as it offers a unique venue for information sharing, indoctrination, recruitment and organisation of attacks.
A particular effort should be made at measuring and predicting the technological capabilities of groups that are likely to radicalise. An attempt should also be made at forecasting

technological evolvement which would lead into more dangerous forms of terrorism and defining early warning signs for such activities. This will enable monitoring of technical capabilities in addition to social driving forces. Main actors that are best positioned to provide early warnings should be identified and best practices and efficiency of existing action plans should be assessed. Alternative approaches and best practices tried out in different European cities, such as cooperation between police, schools and community activities should be looked into.

The research should in addition, address the possible pitfalls or risks of developing early warning indicators. It should integrate in the process ethical and legal issues, including on national level and elucidate in the results the balance between the devised tools and privacy.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Contribution to the 'European Union Counter-Terrorism Strategy' and more particularly to the 'Strategy and Action Plan on Radicalisation and Recruitment' adopted by the Council in December 2005. Actions in this area will improve the understanding of the threats posed by individuals and groups and provide to the local and regional deciders the possibility to adapt prevention measures early to avoid security problems caused by social phenomena leading to terrorism or violent extremism.*

Topic SEC-2010.6.1-2 Develop models and tools to detect and evaluate risks of terrorism

Description of topic:
The task is to propose a methodology for risk assessment of terrorism taking into account the differences between home-grown and imported/exported terrorism. This methodology should address the threats to critical infrastructure, their vulnerability to the threats, and the consequences. The uncertainty of the estimation and the measuring of elements of risks should be balanced across multiple perspectives of terrorism risks. The methodology should then be applied to concrete examples.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Allow the different stakeholders of security to better balance prevention, preparedness and response, and to prioritise and target the use the civil security resources.*

Topic SEC-2010.6.1-3 Reduction of the cognitive biases in intelligence analysis

Description of topic:
Intelligence analysts are involved in analytical processes to assess and react to certain situations. Throughout that analytical process, they might be subject to cognitive biases that may have a negative impact on the quality of the final assessment. The purpose of this topic is: a) to have an exhaustive overview of cognitive biases (synthesis), b) to explore the extent to which cognitive biases can be described and modelled with the objective to reduce the risk

for cognitive biases (feasibility) in analysis and c) to investigate the potential integration of these models into analysis tools in a service oriented open architecture.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Better understanding of cognitive biases and reducing their impact in intelligence analysis will improve the quality of information provided to security decision-makers.*

Area: 10.6.2 Understanding organisational structure and cultures of public users

None

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

The security domain is ‘by definition’ one with broad uncertainty even within the most near-sighted time horizon; foresight studies and scenario building techniques are therefore very much needed for all missions. 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 trade-offs between security and other societal objectives such as the right to privacy and social cohesion.

Topic SEC-2010.6.3-1 Developing a reference framework for the European security culture: the perception of threats and the trust in public authorities and the police and the perception of security as a service

Description of the topic:
The task is to make a cultural and behavioural analysis. As a first step various security cultures throughout Europe should be studied to build a reference framework for the European security culture and to define approaches towards a secure society where citizens perceive security as a service without trade-offs between security and freedom. The risk of surveillance escalation should be addressed and the proposed reference framework should respect privacy and be based on essential security measures, confidence and human respect. Civil society organisations should be represented in the proposed approach and the differences in views between women and men should be analysed.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Give to policy stakeholders a clear view on the kind of security systems that are acceptable by the European citizens. It could also help the deciders understanding better how privacy enhancing technologies could play an important role in the European security.*

Topic SEC-2010.6.3-2 Fore sighting the contribution of security research to meet the future EU roles

Description of the topic:
New tasks are expected to strengthen the EU's role towards providing a comprehensive security approach to its citizens. The external dimension of security may become every more important. The security impact of global climate change needs to be addressed. Furthermore, a stronger common approach to civil protection and crisis management is needed. The task is to develop scenarios as how security research under FP7 and beyond can best contribute to this comprehensive approach while giving due consideration to the ethical and societal dimension.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Provide input for the planning of security research to meet future EU roles beyond those defined in the ESRAB report.*

Topic SEC-2010.6.3-3 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)

Description of the topic:
The task is to develop foresight based methodologies for the rigorous assessment of investment alternatives, intended to prevent or mitigate insecurities with uncertain and potentially catastrophic ramifications. Both financial costs as well as the trade-off between security and other societal objectives, such as the right to privacy and social cohesion, should be addressed.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Provide to the users a decision support system providing them for insight into the pros and cons of specific security investments compared to a set of alternatives taking into account a wider societal context.*

Area: 10.6.4 Security economics

Security economics is the analysis of aggregate risks facing society and economy using rigorous analytical and empirical tools of economics. Policy makers may tend to take imperfect security decisions (e.g. regulations) based on a public perception of (in)security, with an impact to market structures. A singular focus on security or competitiveness would be too narrow; research under this area will offer key insights that will contribute to balancing security and the overall policy objectives. Economic theory in particular can offer key insights, enabling governments to optimise their efforts to enhance security and growth.

Topic SEC-2010.6.4-1 Cost-benefit analysis of the present and future security measures in Europe

Description of topic:
The task is to provide a support tool for analysis of the costs and the benefits of security measures in Europe taking into account the probabilities of these measures. It should be targeted to the policy-makers and should help them in their decision making processes. These could include the analysis of CCTV efficacy and of reliability of terrorist behaviour surveillance, the costs of infrastructure protection, the price of the non-protection scenario, the impact of the security society on the economy. Also, the effects of the European economic stagnation should be taken into account.

Call: Security Research Call 3

Funding Scheme: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *The tool should help policy-makers when they have to make decision on issues which are security related. The costs and the benefits of the different security measures should become more apparent and the decision makers should be better equipped to understand the security consequences of their decisions and thus be in a better position to make the right decisions.*

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 and ethical issues and prioritisation questions, while taking into account a variety of approaches to ethical, social and legal questions based on divergent ethical, religious, historical and philosophical backgrounds. Aspects of social exclusion, lack of social cohesion that may lead leading to the formation of areas of insecurity within Europe may also be considered as well as 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-2010.6.5-1 Review existing codes of conduct, best practises, etc. as to the ethical use of security technologies and the corresponding legal requirements - make recommendations where shortfalls exist

Description of topic:
Ethics challenges need particular attention because of the constant and rapid change of security practices and technologies causes their societal effects to be insufficiently understood. The task is to study existing codes of conduct, practises, etc related to the installation and the use of security technologies in the context of different countries having different ethical, religious, historical and philosophical backgrounds. The existing practises should also be analysed in light of the corresponding legal requirements. Shortfalls should be identified and current ethical framework revised.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *Give to the decision makers a clear view of the state of the art on the ethical and legal use of security technologies and pave the way towards an improvement of the current practices. Security end-users will benefit from a clearer ethical framework.*

Topic SEC-2010.6.5-2 Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules

Description of topic:
The generalisation of surveillance systems collecting massive data raises data protection and integrity issues. However, the scope of surveillance could in most of the situations be focused and targeted to critical parts. The task is to specify how and when smart surveillance should be used and its characteristics to be effective and scalable to rapidly adapt to changing situations. The criteria for data protection and integrity that could be used to verify that surveillance systems and sharing of information is respecting the privacy of the citizens should also be addressed.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *To limit the collection and storage of unnecessary date and to find a balance between data collections needs and data protection and privacy. Such activity will pave the way towards an approach of surveillance where the respect of the privacy of the citizen will be central.*

Activity: 10.7 Security research coordination and structuring

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.

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

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

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

Topic SEC-2010.7.0-1 Networking of researchers for a high level multi-organisational and cross-border collaboration

Description of topic:
An increasingly large number of experts in Europe focus on security research, knowledge and specialisation. However it is sometimes difficult to find and identify the right expertise at the right location and the right moment. Dedicated training actions in the domain of security are relatively scarce in Europe. European security research experts are spread over many EU countries, thus stressing the need to create virtual centres of research competence to network all this expertise. The task is to propose an integration of existing co operations, as well as establishing new ones, in security fields, while at the same time stimulating appropriate training activities. Entities (research centres, stakeholders, end-users) ready to integrate a part of their research activities should become part of this network. This integration should start around some concrete technical projects and aim to a long lasting cooperation based on a joint programme of work leading to the emergence of a 'virtual research centre' in the security domain.

Call: Security Research Call 3

Funding schemes: Network of Excellence

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

Topic SEC-2010.7.0-2 Feasibility study for EU policy on high-level multi-organisational and trans-boundary interoperable field labs and test centres

Description of topic:
Enhancing the infrastructure for testing by defining an EU policy for field labs and test centres in the field of security research via:

- Identifying the present centre’s and labs in the area of security in Europe and their business models
- Identifying the essential parameters for European field-labs and test centres
- Identifying the best way to involve industry, especially SMEs

Call: Security Research Call 3

Funding schemes: Coordination and Support Action (supporting action)

Expected impact: *A European coordinated approach towards establishing an infrastructure of field labs and testing centres. Inventory of current field labs and test centres.*

Topic SEC-2010.7.0-3 Critical and emerging technologies for security

Description of topic:

Identify technology areas needed for security purposes, specifically those where European industry is dependent from other world regions for these technologies due to e.g. non EU patents, technology transfer barriers, or highly classified (dual) technologies. Alternative technological solutions need then to be sought to allow European produced security equipment to be used / sold / deployed worldwide. The aim of this study is also to identify topics within the emerging technologies of the future (10-20 years ahead), which are suitable to set out high risk, high pay-off research priorities. The study should provide an in-depth analysis of different emerging technology areas, identify issues relevant to civil security research and outline recommendations for future research priorities.

Call: Security Research Call 3

Funding schemes: Collaborative Project and Coordination and Support Action (both coordinating and supporting action)

Expected impact: *A list of critical technologies and a plan to deal with these to allow 'non-dependence' for Europe and a list of emerging technologies and a plan to deal with these to set out high risk, high pay-off research priorities.*

Topic SEC-2010.7.0-4 Organisation of a 'security' competition[20]

Description of topic:

The European Commission (EC) is willing to organise a security competition to test innovative solutions in one of the four security missions. Such competitions will also have a significant media dimension, acting as a promoter of user oriented security solutions and of the related impact on society. The proposer will have to prepare various competition scenarios and one of which will be selected by the EC. The proposer will then have to prepare the rules of the competition which will have to encourage out of the box thinking and ensure a level playing field between different types of participants. These rules will have to be approved by the EC. Then the proposer will organise and run the competition itself in cooperation with the EC and the relevant National Authorities. An amount of around EUR 3 million (for example 1.5 M€, 1.0 M€, 0.5 M€) is foreseen as the cumulated total prize for the three first 'winners'.

Call: Security Research Call 3

Funding schemes: Coordination and Support Action (supporting action)

[20] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

Expected impact: *The aim of the competition is to drive progress in security technologies of value to EU's security missions to find the most innovative solutions to technical challenges through competition and cooperation. Participation of independent teams, individual inventors, student groups and private companies of all sizes in security research and development is encouraged. The competition aims to give a very high visibility to the EU Security Research program in the media.*

Topic SEC-2010.7.0-5 Co-ordination of national research programmes in the area of Security research (ERA-NET)

Description of topic:
With a view to ensuring effectiveness and efficiency of the Security theme and also to exploit opportunities outside the Community scope, the task is to support cooperation and coordination of national and where appropriate regional research activities. An ERA-NET should aim to (a) exchange information on the general situation of security research in their countries and define core areas of common interest to prevent duplication and identify synergies; (b) develop common strategies in the core areas and appropriate transparency mechanisms (referring to a joint capability and technology taxonomy, and considering scope and depth of the transparency as well as agreements on protection of intellectual property and handling of classified information); and (c) explore and demonstrate coordinated and/or joint initiatives in the area of Security research.

Call: Security Research Call 3

Funding schemes: Coordination and Support Action (coordinating action)

Expected impact: *Actions will ensure enhanced networking, coordination and co-operation of the Member States and Associated Countries as well as between relevant organisations on the European level. All this which will contribute to the overall impact of the Security theme by making it more effective and efficient and will achieve increasingly harmonised implementation approaches. It will also contribute to the design of future Work Programmes of the Security theme.*

Topic SEC-2010.7.0-6 Trans-national co-operation among NCPs - phase 2

Description of topic:
Based upon the phase 1 NCP project, SEREN, further reinforce the network of National Contact Points (NCP) for the Seventh Framework Programme under Security theme by promoting trans-national co-operation. Existing NCP network services should be further improved to become more efficient and effective.

The action will focus on identifying and sharing good practices. This may entail various mechanisms such as benchmarking, joint workshops, technical training on security specific issues, and twinning schemes. Practical initiatives to benefit cross-border audiences may also be included, such as trans-national brokerage events.

The proposal should include an in-depth mapping of security research national systems and programmes, improved presentation of the mapping in order to leverage the impact of the dissemination of the results. As for the partner search tool, it should be coordinated with CORDIS, or any other tool upon which the Commission agrees.

Special attention will be given to helping less experienced NCPs rapidly acquire the know-how accumulated in other countries. However, the participation as partners to the project should be organised around a number of regional clusters of NCPs.

The Commission expects to receive a single proposal under this heading.

It is expected to fund co-ordination and support action (coordinating action), and a funding of up to an indicative EUR 1.5 million is envisaged. It is expected that the project should last for a maximum of 3 years, and should in any case finish before March 2013.

Call: Security Research Call 3

Funding Scheme: Coordination and Support Action (coordinating action)

Expected impact: *An improved NCP service across Europe, therefore helping simplify access to FP7 calls, lowering the entry barriers for newcomers, and raising the average quality of submitted* proposals*. A more consistent level of NCP support services across Europe. More effective participation of organisation from third countries, alongside European organisations, in line with the principle of mutual benefit.*

III IMPLEMENTATION OF CALLS

Call title: Security Research Call 3

- Call identifier: FP7-SEC-2010-1
- Date of publication: 30/July/2009[21]
- Deadline: 26/November/2009 at 17.00.00, Brussels local time[22]
- Indicative budget: Total call budget **EUR 210.59 million**[23] [24]
  - An indicative **60%** (deviation possible from 50% to 70%) of the budget for topics to be implemented through **Demonstration and Integration Projects** (Areas 1, 2, 3 and 4).
  - An indicative **40%** (deviation possible from 30% to 50%) of the budget for topics to be implemented through **Capability Projects, Coordination and Supporting Activities** (activities 6 and 7), (Areas 1, 2, 4), and **Networks of Excellence** (activity 7).
  - Within the above indicative limits, up to an indicative 3% can be used for *international co-operation*, and up to an indicative 3% can be used for *ERA-NET*.
- Topics called:

Activity/ Area	Topics called	Funding Schemes
10.1 Security of citizens */ 1.2 Integration projects*	*SEC-2010.1.2-1 Information and knowledge management for the prevention of organised crime*	*Collaborative Project*
10.1 Security of citizens */ 1.3 Capability projects*	*SEC-2010.1.3-1 Innovative tools to combat organised crime and terrorism financing and money laundering*	*Collaborative Project*
	SEC-2010.1.3-2 Tackling counterfeit medicines and related criminal networks	*Collaborative Project*
	SEC-2010.1.3-3 Detection of IED manufacturing facilities	*Collaborative Project*
10.1 Security of citizens */ 1.4 Coordination and support actions*	*SEC-2010.1.4-1 Advanced forensic toolbox*	*Coordination and Support Action (coordinating)*
	SEC-2010.1.4-2 Controlling the change of properties of chemicals to preclude misuse	*Coordination and Support Action (coordinating)*
10.2 Security of infrastructures and utilities */ 2.1 Demonstration programme*	*SEC-2010.2.1-1 Security of mass transportation - phase II*	*Collaborative Project*
10.2 Security of infrastructures and utilities */ 2.3 Capability projects*	*SEC-2010.2.3-1 Planning, (re)design, and (re)engineering of urban areas to make them less vulnerable and more resilient to security threats*	*Collaborative Project*
	SEC-2010.2.3-2 Assessment framework and tools to identify vulnerabilities of energy grids and energy plants and to	*Collaborative Project*

[21] The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.

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

[23] Under the condition that the preliminary draft budget for 2010 is adopted without modifications by the budget authority.

[24] The final total budget awarded to this call, following the evaluation of proposals, may vary by up to 10% of the total value of the call.

	protect them against cascading effects	
	SEC-2010.2.3-3 Automatic detection and recognition of threats to critical assets in large unpredictable environment	*Collaborative Project*
***10.2 Security of infrastructures and utilities** / 2.4 Coordination and support actions*	*SEC-2010.2.4-1 New concepts to meet the requirements for the protection of civil/commercial aviation*	*Coordination and Support Action (both coordinating and supporting)*
***10.3 Intelligent surveillance and border control** / 3.1 Demonstration programme*	*SEC-2010.3.1-1 European-wide integrated maritime border control system - phase II*	*Collaborative Project*
***10.3 Intelligent surveillance and border control** / 3.2 Integration projects*	*SEC-2010.3.2-1 Monitoring and tracking of shipping containers*	*Collaborative Project*
***10.4 Restoring security and safety in case of crisis** / 4. 1 Demonstration programme*	*SEC-2010.4.1-1 Aftermath crisis management - phase 1*	*Coordination and Support Action (supporting)*
***10.4 Restoring security and safety in case of crisis** /4. 2 Integration projects*	*SEC-2010.4.2-1 Interoperability of data, systems, tools and equipment*	*Collaborative Project*
	SEC-2010.4.2-2Preparedness and Resilience to a CBRN crisis	*Collaborative Project*
	SEC-2010.4.2-3 Information acquisition using dedicated platforms, including UAV, aerostatic platforms(balloons) and satellites	*Collaborative Project*
***10.4 Restoring security and safety in case of crisis** /4.3 Capability projects*	*SEC-2010.4.3-1 Alert and communication, including role of media, towards the population in crises management*	*Collaborative Project*
	SEC-2010.4.3-2 Adaptation of existing Decision Support Systems (DSS) to new radiological threats	*Collaborative Project*
***10.4 Restoring security and safety in case of crisis** /4.4 Coordination and support actions*	*SEC-2010.4.4-1 Basic service restoration (e.g. energy, water, communication), business continuity, domestic/ environmental normality*	*Coordination and Support Action (coordinating)*
***10.6 Security and society** / 6.1 Citizens and security*	*SEC-2010.6.1-1 Signs of 'early warning' to detect trends and weak signals in social polarisation, radicalisation development and segregation*	*Collaborative Project / Coordination and Support Action (both coordinating and supporting)*
	SEC-2010.6.1-2 Develop models and tools to detect and evaluate risks of terrorism	
	SEC-2010.6.1-3 Reduction of the cognitive biases in intelligence analysis	
***10.6 Security and society** / 6.3 Foresight, scenarios and security as an evolving concept*	*SEC-2010-6.3-1 Developing a reference framework for the European security culture: the perception of threats and the trust in public authorities and the police and the perception of security as a service*	

	SEC-2010.6.3-2 Fore sighting the contribution of security research to meet the future EU roles	
	SEC-2010.6.3-3 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)	
10.6 Security and society *\/ 6.4 Security economics*	*SEC-2010.6.4-1 Cost-benefit analysis of the present and future security measures in Europe*	
10.6 Security and society *\/6.5 Ethics and justice*	*SEC-2010.6.5-1 Review existing codes of conduct, best practises, etc. as to the ethical use of security technologies and the corresponding legal requirements - make recommendations where shortfalls exist*	
	SEC-2010.6.5-2 Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules	
10.7 Security research coordination and structuring	*SEC-2010.7.0-1 Networking of researchers for a high level multi-organisational and cross-border collaboration*	*Network of Excellence*
	SEC-2010.7.0-2 Feasibility study for EU policy on high-level multi-organisational and trans-boundary interoperable field labs and test centres	*Coordination and Support Action (supporting)*
	SEC-2010.7.0-3 Critical and emerging technologies for security	*Collaborative Project / Coordination and Support Action (both coordinating and supporting)*
	SEC-2010.7.0-4 Organisation of a "security" competition	*Coordination and Support Action (supporting)*
	SEC-2010.7.0-5 Co-ordination of national research programmes in the area of Security research (ERA-NET)	*Coordination and Support Action (coordinating)*
	SEC-2010.7.0-6 Trans-national co-operation among NCPs - phase 2	*Coordination and Support Action (coordinating)*

- **Eligibility conditions**

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

  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.

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

Funding scheme	**Minimum conditions**
Collaborative projects[25]	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Network of Excellence	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (coordinating action)	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (supporting action)	At least 1 independent legal entity

Proposals containing any classified information shall be declared ineligible.

- **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 EPSS. The Commission will instruct the experts to disregard any pages exceeding these limits. The minimum font size allowed is 11 points. The page size is A4, and all margins (top, bottom, left, right) should be at least 15 mm (not including any footers or headers).

  A one-stage submission procedure will be followed.

  Proposals will be evaluated in a single-step procedure.

  Proposals may be evaluated remotely.

- **Indicative timetable:** This call in 2009 invites proposals to be funded in 2010. Evaluations of proposals are expected to be carried out in January/February 2010. It is expected that the grant agreement negotiations for the short listed proposals will be opened in the first half of 2010.

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

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

  Classified Information

[25] The funding scheme **Collaborative project** will in this Call be divided into demonstration programmes (one or a number of individual projects) (large scale integrating projects with indicative Community funding of over EUR 20 000 000), integration projects (large scale integrating projects with indicative Community funding of over EUR 3 500 000) and capability projects (small and medium-scale focused research projects with indicative Community funding of EUR 3 500 000 and below).

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

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

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

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

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

Ethical Review

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

Small and Medium Enterprises (SME) and end-users

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

Evaluation

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

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

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

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

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

  Proposers claiming that their proposal should receive Community **funding up to 75%** (for research activities) should demonstrate in the proposal that the exceptional required conditions (very limited market size and a risk of "market failure", the need for accelerated equipment development in response to new threats) apply.

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

Indicative budget allocation for the Security Work Programme 2010

A total of EUR 220.47 million[26] is to be committed from the 2010 Community budget. The indicative budget allocation is given in the below table. More information will be provided on http://cordis.europa.eu/fp7/calls/.

Call/activity	2010 EUR million
Call FP7-SEC-2010-1	**210.59**
General Activities (cf. Annex 4)	**2.23**
Other Activities: • Expert Evaluators (EUR 1.4 million) • Calls for tender (EUR 0.4 million) • Support to conferences; impact assessment; monitoring, information / communication; studies etc (EUR 1.0 million) • Competition prize (EUR 3.0 million) • Support to SRC'10 (EUR 0.22 million)	**6.02**
Estimated total budget allocation	**220.47**[27]

Summary of budget allocation to general activities for 2010 in million EUR (cf. Annex 4)

Cordis	0.42
Eureka / Research Organisations	0.02
COST	1.73
ERA-NET	0.06
Total	**2.23**

[26] Under the condition that the preliminary drat budget for 2010 is adopted without modifications by the budget authority.

[27] Of which € 1.63 million is foreseen to be reserved for the forthcoming Commission proposal on Metrology.

IV OTHER ACTIONS[28]

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

- **Call for tender for public procurement**[29] on 'State of the art of standardisation and certification in the Security domain'[30] will be issued by the Commission (in close coordination with the Programme Committee of national representatives), where appropriate.

  In order to answer to the ESRAB report, the EC is seeking to understand better the standardisation landscape in the security area as well as the certification activities which may already exist. Related domain like "Information security" may be used as a starting point for this work. Next steps will be to derive from the existing standardisation and certification activities a research/policy agenda in order to shape the future for the standardisation and certification in the security area. The aim is to ensure the quality of the security solutions embedded in various security products or system, to give higher confidence in security products/systems to the EU citizens and EU businesses and to improve the competitiveness of the EU security industry. The procedure is scheduled for the first and second quarter of 2010.

  Funding scheme: Coordination and Support Action - public procurement

- **'Support to the Belgian Presidency European Security Research Conference – SRC'10'**[31]

  The Belgian presidency is hosting the "European Security Research Conference – SRC'10". The objective is to support the conference, which aims at disseminating information on activities of FP7 Security Research (including information seminars, audiovisual aids, exhibitions, competitions, etc and bringing together the main European players of research and development in the field of security.

  The named beneficiary for the grant is:
  BELSPO (Belgian Federal Science Policy Office)
  Rue de la Science 8
  1000 Brussels
  Belgium

  The EC contribution is limited to EUR 220 000 and will not represent more than 50% of the total cost of the conference.

  The EC contribution will be implemented as a grant through a support action to the named beneficiary. It will be evaluated in accordance with the standard FP7 evaluation criteria

[28] 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).

[29] Call for tender can also be attributed via a framework contract.

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

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

(including weight and thresholds) and sub-criteria, together with an eligibility, selection and award criteria for the funding scheme as set out in Annex 2 of this work programme.

Funding scheme: Coordination and Support Action - named beneficiary

- 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.

  Funding scheme: Coordination and Support Action - expert appointment letters

- **Monitoring, evaluation and impact assessment**: The Security research theme will comply with the requirements for monitoring, evaluation, and impact assessment. This may involve studies and surveys (implemented through public procurement) as well as panels of nominated experts.

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

V INDICATIVE PRIORITIES FOR FUTURE CALLS

Indicative roadmap for publication of future calls

07/2010:	Security Research Call 4
07/2011:	Security Research Call 5
07/2012:	Security Research Call 6

Indicative approach of future calls

- **Security Research Call 4** will be open for the *second phases* of the demonstration projects[32] called for in Security Research Call 2 and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

- **Security Research Calls 5 and 6** will offer reserve opportunities for the second phases of the demonstration projects called for in Security Research Calls 1 and 2, in case no proposal will have been selected for funding in earlier calls, and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

All calls will follow the **building block approach** of the Security theme. While focussing on the demonstration projects, these will be supported and enabled by the output of the capability and integration projects.

[32] If required, additional calls to the main annual calls can be launched especially with a view to the second phases of demonstration projects.