WORK PROGRAMME 2007-2008

COOPERATION

THEME 10

SECURITY

(European Commission C(2007)2460 of 11 June 2007)

<u>Changes to the Cooperation Work Programme: Security Theme</u>

This work programme replaces the version adopted on 26 February 2007.

The only substantive modifications that have been made to the content are as follows:

- **Pages 42 and 44: Addition of 76,2 M€ from the 2008 budget to Call FP7-SEC-2007-1**

- **Pages 42 and 49: Addition of 20 M€ from the 2008 budget to Call FP7-ICT-SEC-2007-1**

THEME 10: SECURITY

Table of contents

THEME 10: SECURITY

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 acts of terrorism and (organised) crime, natural disasters and industrial accidents 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 co-operation of providers and users for civil security solutions; to improve the competitiveness of the European security industry and to deliver mission-oriented results to reduce security gaps.

The Security theme will maintain an exclusively civil orientation and focus on activities of clear European added value.

This 2007 security research Work Programme has been given an emphasis towards research activities related to border security and to the security of critical infrastructures and utilities.

I   CONTEXT

Policy context

As a primary policy context, the Security theme provides contributions to the implementation of EU external policy[1], for creating an EU-wide area of justice, freedom and security[2], and for policy areas such as transport[3], health[4], civil protection[5] (including natural and industrial disasters), energy[6] and environment[7].

A secure European framework is the basis for planning our lives, for economic investments, for prosperity and freedom. Thus the Security theme *in a secondary policy context* also contributes to growth and employment in general and the competitiveness of European industry.

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

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

---

[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;*

Community initiatives and avoid duplication (e.g. with the 'Framework Programme on Security and Safeguarding Liberties': Actions under the Security theme are rather methodology and technology oriented, while the mentioned Framework Programme focuses on actions related to policy and operational work in the area of law enforcement and combating and preventing crime/terrorism).

Approach

The following paragraphs explain the underpinning logic of how the Security theme is organised with respect to structuring its scope and content as well as to sequencing the content in a series of Work Programmes. Experience and consultations of the Commission's *Preparatory Action for Security Research* (PASR, 2004-2006)[8] are also taken into account.

Scope and content of the Security theme

Following the recommendations of the Commission's *European Security Research Advisory Board (ESRAB)[9]*, 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 organised in 11 **functional groups**[10] - of the persons and organisations responsible for safeguarding security in these mission areas by funding the research that will deliver the required **technologies and knowledge** to build up these capabilities. It is clear however, that "technology itself cannot guarantee security, but security without the support of technology is impossible" and that the use of security related technologies must always be embedded in political action. To support such action and also to improve the effectiveness and efficiency of the technology related research, three domains of cross-cutting interest were selected as well:

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

---

[8] *COM(2004)72; http://cordis.europa.eu/security/;*
[9] *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.*
[10] *For complete list of functions see chapter IV. Research with relevance for the security capabilities is also done elsewhere in the Framework Programme or outside.*

Ambition and theme architecture: Routes to meet the objectives

The Security theme aims at **meeting its main objectives** – improved security for the citizens, enhanced competitiveness for industry - **as substantiated in the topics of its 'demonstration projects' 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.

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 top level of the building block structure, **demonstration projects** 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 projects will be implemented in two phases:

  Phase 1 with a duration of 1 – 1,5 years will define their strategic roadmaps and trigger EU wide awareness, both elements involving strategic public and private end users as well as industry and research. The strategic roadmaps will take into account

Figure 1: Research routes to meet the Security theme objectives

relevant completed, ongoing and planned work and indicate further research needs for Security theme integration projects and capability projects, but as well for other themes of the 7th Framework Programme or for the national level. The funding scheme that applies to demonstration projects phase 1 is *coordination and support actions*.

Phase 2 will then technically implement the system of systems demonstration projects, taking already into account steps which have to follow the research like standardisation, development of marketable products and procurement. This will mobilise a significant volume of resources, the typical duration is up to 4 years. The funding scheme that applies to demonstration projects phase 2 is *collaborative projects*.
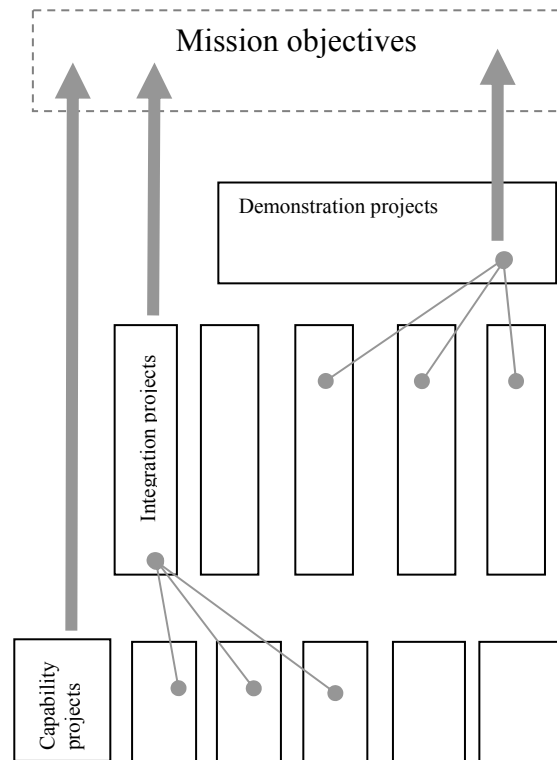
- On the medium level of the building block structure, **integration projects** aim at mission specific combination of individual capabilities providing a security *system* and demonstrating its performance. They depend upon the technology and knowledge building blocks carried out within the capability projects or elsewhere. Their average duration is 4 years. The funding scheme that applies to integration projects is *collaborative projects*.

- 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*. In many cases these will also have cross-mission relevance. Their average duration is 2-4 years. The funding scheme that applies to capability projects is *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, and society relevant research issues can also be integrated in technology projects. Concerning activity *Security systems integration, interconnectivity and interoperability collaborative projects* are regarded as the appropriate funding scheme, with characteristics and sizes comparable to the capability projects.

Collaborative projects can be chosen as funding scheme for *Security and society* actions, but *coordination and support actions* apply as well. For activity *Security Research coordination and structuring*, the most appropriate funding scheme will be *coordination and support actions*. Core activities will be studies; networking; exchanges of personnel; exchange and dissemination of good practices; the definition and organisation of joint or common initiatives; meetings, conferences and events etc. and the management of the action.

The use of *Networks of Excellence* and *Joint Technology Initiative* funding schemes is not foreseen at this stage.

Concerning the *collaborative project* funding scheme in the Security theme, the Community funding 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.[11] If proposers wish to claim this higher funding level, it will be their task to demonstrate in their proposal that the required conditions apply. The final decision will be based on the recommendations of the relevant evaluation panel.

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

---

[11]*Decision 1906/2006/Ec of 18/12/2006 on the rules for participation, Art 33.1*

Principles and characteristics of Security theme actions

This Security theme has high political relevance both for security related and economic policy areas (growth, employment etc.). While building on a strategic research agenda, it is always open for well justified **unforeseen policy needs**. It should also support the (re)structuring of the European security sector.

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. With a view to the Security theme's objective of increasing the competitiveness of industry, the broad **involvement of SMEs** in consortia is highly encouraged. The performance and integration of SMEs is furthermore supported through dedicated measures, in particular SEC-2007-7.0-01, SEC-2007-7.0-05 and SEC 7.0-06. 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 other 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 consortia is considered of utmost importance.

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 take-up of existing and emerging technologies for the civil security sector. Recognizing that Security research covers areas of **dual use** technology relevant to both civilian and military applications, coordination with the *European Defence Agency* (EDA), who will consult its Member States about national programmes, will ensure complementarity wherever necessary.

Actions within the Security theme build not only on technology gain from the capability projects, and also on research outcomes of other themes of the 7th Framework Programme or of national research programmes. Only issues of **European added value** are covered in the theme and it is ensured that it is complementary with all other Community actions. Complementarity with non-EU research will be ensured via the members of the Security Programme Committee configuration.

In general, a network of National Contact Points and in particular network(s) of security research stakeholders (including both the supply and the user side) are seen as instrumental in promoting the **dissemination** of security research to its end users, national public authorities and citizens alike. Suitable Coordination and support actions to achieve this could also receive funding (see in particular topics in activity 7).

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. Special provisions will be taken in the grant agreement.

For the Security Research Call 1, proposals must not contain any **classified information**. This would lead to declaring them ineligible immediately. However, it is possible that the output of

---

[12] *COM(2005)705; Article 22*

an action needs to be classified or classified inputs are required. In this case proposers have to ensure *and provide evidence* of the clearance of all relevant persons and facilities. Consortia have to clarify issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal. Proposals need to provide a *security aspect letter,* indicating the levels of classification required. Appropriate arrangements have to be included in the consortium agreement.

All actions of the Security theme are in principle open to **international co-operation** to Industrialised countries as well as to ICPC[13] countries. However, according to the *Specific Programme, parts of the Work Programme can be* restricted to EU and associated countries. Such restriction is not foreseen in the 2007 Work Programme. At this stage, it is also not foreseen to have any 'specific international co-operation actions' in the Security theme.

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.

Ethical principles and **gender aspects** must always be taken into account. 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. Therefore, a balanced representation of women and men at all levels in research projects is encouraged.

Cross-thematic approaches: For all four missions, security is often linked to the interoperability of systems (e.g. for command & control, networked critical infrastructures, border management & security etc.); and often interoperability is an ICT issue. Thus, a Joint Call for Proposals with Theme 3 *Information and Communication Technologies* is foreseen in 2007 in order to ensure comprehensive coverage.

Security issues could also be regarded as intrinsic elements of several of the other *Co-operation* themes. The scope of the calls has been carefully defined throughout the themes, in order to avoid gaps or duplication (with a view to the full duration of the 7th Framework Programme, not only the Security Research Call 1). 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.

Risk-sharing Finance Facility

In addition to direct financial support to participants in RTD actions, the Community will improve their access to private sector finance by contributing financially to the **'Risk-Sharing Finance Facility' (RSFF)** established by the European Investment Bank (EIB).

The Community contribution to RSFF will be used, by the Bank, in accordance with eligibility criteria set out in the Work Programme 'Co-operation' (horizontal issues). RSFF

---

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

support is not conditional on promoters securing grants resulting from calls for proposals described herein, although the combination of grants and RSFF-supported financing from EIB is possible.

In accordance with the Specific Programme 'Co-operation', which stipulates that the Community contribution to RSFF will be funded by *proportional contributions of all Themes, except Socio-economic Sciences and the Humanities*, the Commitment Appropriations for this Theme to RSFF in 2007 will be 4,428 M€. This amount will be committed entirely in 2007.

The use of the Community Contribution from the Specific Programme 'Co-operation' will be on a 'first come, first served' basis and will not be constrained by the proportional contribution of Themes.

Further information on the RSFF is given in the Annex 4 of this work programme.

Other activities

The theme will support **ERA-NET** activities[14] that 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.

ERA-NET projects can network four types of activities: (1) Information exchange – (2) Definition and preparation of joint activities – (3) Implementation of joint activities – (4) Funding of joint trans-national research actions:

- ERA-NETs launched under FP6 wishing to submit a follow-up proposal under FP7 have to propose a strong coordination action focusing directly on steps three and four, in order to achieve mutual opening and trans-national research via joint/common calls, joint/common programmes or, if appropriate, other joint trans-national actions.

- New ERA-NETs, which address new topics and without any experience from FP6, should address at least the first three steps, but are encouraged to aim at the "four step approach", as described above.

The Security Research Call 1 offers the possibility to submit a dedicated ERA-NET proposal under *Topic SEC-2007-7.0-04 Transparency and networking amongst Member States and Associated Countries.*

---

[14] *ERA-NET activities will be subject to a joint call across the Specific programme 'Co-operation' - see Annex 4.*

II   CONTENT OF CALLS IN 2007

II.1   Security Research Call 1 (FP7-SEC-2007-1)

The primary ambition of the Security theme is to provide 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.

Thus the Security Research Call 1 launches the implementation of two demonstration programmes (phases 1) in the two security policy missions *Security of infrastructures and utilities* and *Intelligent surveillance and border security.* They will demonstrate integrated innovative systems of systems (focus on highest level building block).

In parallel, and supporting this focus from the other building block levels, novel and improved technologies will 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.

Topic descriptions are deliberately kept rather brief and general in order to allow for a variety of promising technological approaches which may address more than one *specific* security application. This ensures that in principle more than one proposal can be selected for each topic, thus guaranteeing competition amongst proposals. It is also possible *not* to select any proposals submitted to a topic at all, if the quality is not sufficient and evaluators do not recommend it.

The Security Research Call 1 is open to the submission of proposals for actions referring to the following topics.

Activity 1: Increasing the *Security of citizens*

The challenge of this activity is to contribute to combating the activities of organised crime (such as drug and weapons smuggling, complicated money laundering and child pornography trafficking schemes, individual and private sector fraud, illegal movement of equipment, technology and knowledge etc.) and terrorism by developing secure information and financial networks, robust secure communications and virtual policing of information infrastructures, including the internet, to uncover and track terrorist activities; to enhance the intelligence and analysis capabilities (capacity and quality) across a range of sectors in concert with digital forensic technology to track, trace and apprehend terrorists; with respect to terrorist weapons to detect, track, trace, identify and neutralise CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) – both 'traditional' and 'home grown'. Speed, robustness and affordability will be the driving design parameters for technological and system solutions.

Area 1.1: Demonstration projects

No demonstration programmes foreseen in this activity for Security Research Call 1. See also chapter IV *Indicative priorities for future calls*.

Area 1.2: Integration projects

Expected impact: *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces. In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

The Security Research Call 1 calls for the following actions:

Topic SEC-2007-1.2-01 Intelligent urban environment observation system

Technical content / scope: The task is to develop both a fixed and a man portable, integrated, fast, wide area behavioural observation system for individuals, platforms and goods in complex (urban) environments. It should meet surveillance and security tasks including compound security, trafficking of illegal goods, safety monitoring and evacuation on a 24h / 7 days basis. This will include the integration of sensor technologies, data fusion and intelligent observation systems to enable stand-off detection and analysis through barriers, of substances and weapons, of carriers and people as well as behaviour analysis to separate potential perpetrators from crowds and neutralise the threat.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-1.2-02 Integrated mobile security kit

Technical content / scope: The task is to develop an innovative and integrated, mobile security kit for rapid deployment, which can be applied to various situations such as large scale events (e.g. sport or show events) and to early warning / crisis response. The aim is to support and enhance the flexibility and adaptation capabilities of European security forces for preventing or responding to security incidents. This will involve sets of mobile security modules; tools for the protection of special persons; general security of events; interfacing with local security forces; multiple sensors etc.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Area 1.3: Capability projects

Expected impact: *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

The Security Research Call 1 calls for the following actions:

Function: Detection, identification & authentication

Topic SEC-2007-1.3-01 Stand off scanning and detection of hidden dangerous materials, objects or stowaways, fast and reliable alerting and specification.

Technical content / scope: The task is to develop stand off large throughput scanning capabilities required to pick out from a stream suspect items, such as drugs, viri, CBRNE (chemical, biological, radiological and nuclear substances as well as explosives), hidden objects or persons, including both fast narrow scanning in specific streams, and wide area scanning with sufficient granularity to enable law enforcement to intervene. The steps to take will be (a) very fast alerting with low false alarm rates on a broad class of objects and substances, (b) after the alarm and within reasonable time identification of a type of substance and (c) very thorough analysis and profiling on the biological or chemical components of specific substances.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-1.3-02 Improved control of explosives throughout their "lifecycle"

Technical content / scope: In order to prevent the use as terrorist weapons of commercial explosives and detonators as well as of improvised substances made from widely available precursor chemicals, the task is to tag explosive characteristics of precursor compounds to be able to tag, trace and detect more readily components and detonators and to develop smart secure detonators; to investigate into secure stockpiling, use and transport of explosives.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Positioning & localisation

Topic SEC-2007-1.3-03 Localisation and tracking of components of substance production

Technical content / scope: With a view to either preventing production or detecting production and use, the task is to develop novel technologies and innovative approaches for the monitoring of the production, trade, availability and use of chemical components required for the production of certain types of drugs, explosives and agents.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-1.3-04 Observation through water, metal, ground etc

Technical content / scope: The task is to develop novel technologies and innovative approaches enabling the observation of people, platforms and carriers in complex environments in order to increase surveillance and intervention capabilities. Increasing the surveillance area and performance of future sensor systems should address the lowering of successive obstacles (people, buildings, metal, water, vegetation) that currently inhibit the observation.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Situation awareness & assessment (surveillance)

Topic SEC-2007-1.3-05 Water distribution surveillance

Technical content / scope: The task is to further improve the surveillance of water distribution networks for security purposes with respect to the following issues: Design of methodologies to identify new relevant contaminants; modelling of the impact of contamination (preventive and real-time); adaptation and integration of various sensors in a surveillance system; development of tools for the optimal configuration of sensors in a distribution network; tools for the neutralisation of contaminants including the development of methods to decontaminate polluted lines and installations; development of systems for data handling from various sources like sensors, customer information, health complaints, process control, intelligence services and decision support tools. Ongoing actions in particular on the European level need to be taken into account.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-1.3-06 Secure strategic information management systems

Technical content / scope: The task is to create secure situation awareness systems contributing to combating the activities of organised crime, such as drug and weapons smuggling, complicated money laundering and child pornography trafficking schemes, individual and private sector fraud etc., by automatically combining data from disparate high

volumes data repositories (e.g. financial, demographic, mobility, law enforcement data sources etc.) and analysing the data to allow complex conclusions to be generated in order to facilitate appropriate, fast and responsible decision making to prevent or respond to security incidents. Legal restrictions must of course be respected. This will include automated analysis of complex and different cultural/domain data with multiple reference models; the ability to handle and combine real-time data feeds and historical databases; the policing of existing information systems. The security of the infrastructure to perform this task is also a key objective.

Call: Security Research Call 1

Funding scheme(s): Collaborative project.

Activity 2: Increasing the *Security of infrastructures and utilities*

The challenge of this activity is to protect critical infrastructures and utilities (both physical and logical systems from e.g. sensitive and administrative buildings (often also of symbolic value), train and subway stations, sensitive manufacturing plants, energy production sites, storage and distribution, to information and communication networks or public events etc.) against being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. Their direct, often trans-national dependencies and the cascading failures generated in case of failure in one of them (special emphasis is given to the robustness of the power transmission and distribution system due to its underlying operational importance to most others) will be taken into account, as well as the consequential dependencies to the commercial environment. Cost effectiveness will be addressed as one of the driving design parameters. Efficient technological solutions need to be developed. Where no solution exists, the research effort should emphasise low cost solutions; where efficient but costly technologies exist, research efforts should focus on ways to reduce dramatically the cost for similar performances.

Area 2.1: Demonstration projects

Topic SEC-2007-2.1-01. Security of critical infrastructures related to mass transportation (phase 1)

The Security Research Call 1 calls for the *first phase* of this demonstration programme, which will define its strategic roadmap and ensure EU wide awareness.

The scope and technical content of the full demonstration project (phase 2, which will build upon phase 1) will be the demonstration of a consistent and integrated set of mass transportation security systems to secure transport networks, nodes and platforms, taking into account the specific requirements for each sector/mode and the particular cross-border dimension of mass transport. This covers

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

- Interoperability of different surveillance 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;

- Post-event situation analysis systems capable of rapidly accessing and piecing together different multi-media and digital data to re-enact a sequence of event;

- Common operational picture integrating and displaying data from a diverse set of sources on optimised man machine interfaces utilising intelligence based alarm management;

- Neutralisation and containment systems for attack avoidance, suppression or nullification.

The interoperability requirements will drive standardisation in this area.

Scope of Phase 1 (open): The action will define the strategic roadmap required for the demonstration project 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 project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the co-operation of third country participants is required or recommended.

Call: Security Research Call 1
Funding schemes: Coordination and support action (aiming at supporting research activities).

Expected impact: *Through comprehensive preparation (not proposal preparation) of the demonstration project, the action will provide a solid basis for the description of its phase 2 in the Work Programme of Security Research Call 3 in 2009 as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified EU wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration project 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 EU 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 2.2: Integration projects

Expected impact: *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces. In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

The Security Research Call 1 calls for the following actions:

Topic SEC-2007-2.2-01 Integrated protection of rail transportation

Technical content / scope: The task is to develop an integrated system to improve the security of rail transportation through better protection of railways and trains, and to reduce disparity in security between European railway systems. This will include the immunity of signal and power distribution systems against electromagnetic terrorism, the detection of abnormal objects on or under ballast; clearance of trains before daily use; control of access to driver's cabin, detection of unauthorised driver; new methods/tools to isolate and secure luggage; as well as a study and tools to reduce disparity of European railway systems' security. The action will demonstrate the potential of the European rail transportation systems for improved protection and homogeneity.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Area 2.3: Capability projects

Expected impact: *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

The Security Research Call 1 calls for the following actions:

Function: Detection, identification & authentication

Topic SEC-2007-2.3-01 Detection of unattended goods and of owner

Technical content / scope: In the framework of a public area under video surveillance, the task is to develop novel tools and innovative approaches to (a) the automated real-time detection of the fact that goods (typically luggage) have been abandoned, (b) the fast identification of the individual who left the goods, and (c) the fast determination of the current location of that individual or his/her followed path.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-2.3-02 Detection of abnormal behaviour of vehicles both in wide and small land areas

Technical content / scope: (a) Within small, well controlled land areas such as in the proximity of a critical infrastructure under video surveillance or (b) in open land areas which may be relatively cluttered but well controlled with radar sensors, image and pattern processing technology and human behaviour analysis and modelling, the task is to develop novel tools and innovative approaches to automated real-time detection of abnormal behaviour of vehicles (such as suspect trajectory, unusual speed, unexpected manoeuvring etc.). Platforms should supplement existing surveillance systems and be capable of detecting, recognising and classifying movements within areas and also be capable of interfacing to e.g. acoustic, seismic, passive infra red and chemical / biological sensors and video.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-2.3-03 Detection of abnormal behaviour

Technical content / scope: The task is to create novel tools and innovative approaches for the reliable and effective automatic and real-time detection of potentially threatening abnormal behaviour of individuals in a crowd or of a group of individuals in a crowd in an open space, e.g. those in relation to large scale events. This will include the definition of the 'abnormal behaviour' to be detected; deployment of various sensors types; development of solutions applicable for short and mid-range distance. Privacy and civil liberties of individuals must be respected.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Situation awareness & assessment (surveillance)

Topic SEC-2007-2.3-04 Small area 24 hours surveillance

Technical content / scope: The task is to develop novel technologies and innovative approaches enabling for permanent monitoring and surveillance (human beings, vehicles, goods) of the inside and of the surrounding areas of critical infrastructures as well as for permanent information acquisition and information treatment for detection of alert situations. Solutions must be operational on a 24h basis, under all weather conditions.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Activity 3: *Intelligent surveillance and* enhancing *border security*

The challenge of this activity is to address border security in the context of integrated border management ensuring legitimate trade and flow of people, thus supporting the Schengen co-operation, the efforts of national authorities and those of the European Union's external borders agency FRONTEX with respect to the convergence of information management systems, interoperability, training and cascading best practice. Actions will refer to issues relevant for all the consecutive tiers of the *European border security strategy*[15]. The link to standardisation, regulation and legislation as well as to related testing, evaluation and certification will be crucial. The focus of this Work Programme is on illegal immigration as well as on trafficking of drugs, weapons and illicit substances. With respect to illegal immigration the objective is to develop novel, reliable and scaleable solutions to efficiently identify illegal movements, whilst not unduly impeding the flow of the vast majority of legitimate travellers and vehicles. Naturally, privacy and human rights will need to be taken into account. With respect to the trafficking of drugs, weapons and illicit substances such as CBRNE (Chemical, Biological, Radiological, Nuclear and Explosives) agents, the objective is to create a coordinated and integrated security system to ensure the security of goods supply chains and logistics networks, while addressing traceability, standardisation and more affordable robust solutions as well as reduction of unit cost and screening times.[16]

Area 3.1: Demonstration projects

Topic SEC-2007-3.1-01 Integrated border management system (phase 1)

The Security Research Call 1 calls for the *first phase* of this demonstration programme, which will define its strategic roadmap and ensure EU wide awareness.

The scope and technical content of the full demonstration project (phase 2, which will build upon phase 1) will be the demonstration of a comprehensive and integrated border management system relating to the Schengen co-operation and the European Union's external borders capable of providing concentric layers of protection from pre-entry control measures through to co-operation inside and between Member States and Associated Countries. This comprises:

- Surveillance systems to improve situational awareness and detect anomalous behaviour of people and platforms (vehicles, boats, aircraft);

- Identity management systems including documentation, equipment and supporting databases to accurately identify and authenticate individuals, goods and platforms;

- Information management systems to fuse data from disparate systems (identity management, intelligence etc.) in order to improve decision making;

---

[15] As part of the definition of the EU Border Management Strategy , see Council Conclusions of Justice Home Affairs Council of 20-22 September 2006.

[16] Actions under this activity can take up solutions provided e.g. by GMES (see theme 9 Space) or Galileo (see theme 7 Transport (including Aeronautics)).

- Secure communication systems for improved co-operation between national and international border control authorities;

- Positioning and localisation systems to track and trace individuals, goods and platforms;

- Advanced training methods, tools and systems based on true representation simulation systems;

- Improved architectures, processes and systems for border security including extending the legal borders to departure points outside of the EU perimeter.

For the demonstration project to be effective, widespread deployment is required, for which innovative business models will be needed.

Scope of Phase 1 (open): The action will define the strategic roadmap required for the demonstration project 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 project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the co-operation of third country participants is required or recommended.

Call: Security Research Call 1
Funding schemes: Coordination and support action (aiming at supporting research activities).

Expected impact: *Through comprehensive preparation (not proposal preparation) of the demonstration project, the action will provide a solid basis for the description of its phase 2 in the Work Programme of Security Research Call 3 in 2009 as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified EU wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration project, 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 EU 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 3.2: Integration projects

Expected impact: *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This

will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

The Security Research Call 1 calls for the following actions:

Topic SEC-2007-3.2-01 Main port area security system (including containers)

Technical content / scope: The task is to create an integrated port area (land, sub-surface, water) security system capable of providing accurate situational awareness, based on various sources and integrating all result streams, and alerting security operators to required interventions, while doing uninterrupted logistics business. The system will improve situation awareness at main ports through the monitoring and tracking of complex port environments as a consequence of the continuous arrival and departure of cargo (containers), ships, vehicles, staff and passengers, and also the potential threats by boats and swimmers etc. This will include mobile and fixed detection and recognition systems in order to provide intelligent event detection, supporting the decision control; investigation into cargos scanner outputs fused with shipping manifest information, external risk assessment and a-priori threat knowledge which allows for automatic anomaly detection.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-3.2-02 Unregulated land borders and wide land surveillance system

Technical content / scope: The task is to develop an integrated, adaptable land border and large area (including rough or devastated environments) surveillance system. It will be able to detect and locate (the movements of) individuals, vehicles, and hazardous substances (e.g. CBRNE) crossing unregulated land borders and, when required, track and trace their movements thereafter. It will combine novel dedicated remote or autonomous platforms equipped with multi-sensor data acquisition systems (of different types such as chemical and biological) with active imaging (such as radar, infrared, visible). These data will be further processed and integrated, e.g. including their fusion with navigation information and terrain databases. A central display system will present the large amounts of information in an easily managed format that facilitates the priorisation of alarm events, tracks responses, records events for future analysis and supports the human interface with Security personnel.

The capacities offered by the GMES[17] services developed by the *Space* theme will be fully exploited.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

---

[17] *Global Monitoring of Environment and Security*

Topic SEC-2007-3.2-03 Integrated check points security

Technical content / scope: The task is to create an advanced integrated check point system to enhance the performance of the existing screening portals at regulated border crossing or other comparable checkpoints for individuals, vehicles and platforms. This will include advanced detection technologies for threats (e.g. weapons, CBRNE). Detection will be integrated with automatic video analysis systems, multi-biometrics and mobile OCR technologies. Eventually a shared database of information / intelligence between the European border security operators will improve situation awareness. The system shall respect the privacy and civil liberties of individuals.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Area 3.3: Capability projects

Expected impact: *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

The Security Research Call 1 calls for the following actions:

Function: Detection, identification & authentication

Topic SEC-2007-3.3-01 Air 3D detection of manned and unmanned platforms

Technical content / scope: In order to cover a region (including extended border lines and large areas) 24 hours a day in all weather conditions, the task is to develop a three dimensional air surveillance system capable to identify all kinds of manned and unmanned platforms. This will include non-cooperative target recognition, utilizing active and passive sensors on airborne platforms and/or earth observation capacities.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Situation awareness & assessment (surveillance)

Topic SEC-2007-3.3-02 Surveillance in wide maritime areas through active and passive means

Technical content / scope: The task is to develop novel, automatic surveillance capabilities through manned and unmanned platforms (land / sea / air / space), equipped with several sensors and sophisticated data fusion processes. This could involve the combination of tracing technologies, digital signal processing, image and pattern processing with data and information management.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Communication

Topic SEC-2007-3.3-03 Solutions for ensuring disruption-tolerant end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems

Technical content / scope: The task is to develop suitable novel communication services which guarantee the required quality of service and data integrity making use of multimode communication solutions, even in the face of disruptions that may occur due to security incidents. These will mainly be focused on wireless/mobile communication making use, where appropriate, of disruption-tolerant networking schemes. Solutions should include appropriate end-to-end and hop-by-hop security features for voice, data information and access.

Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Activity 4: *Restoring security and safety in case of crisis*

The first challenge of this activity is to ensure that governments, first responders and societies are better *prepared* prior to unpredictable catastrophic incidents using new, innovative and affordable solutions. The second challenge is to improve the tools, infrastructures, procedures and organisational frameworks to *respond and recover* more efficiently and effectively both during, and after, an incident.

Three areas are to be addressed, namely incidents caused by: (1) terrorist acts and (organised) crime, including the use of conventional explosive weapons and weapons of mass destruction and disruption (e.g. CBRNE); (2) natural disasters including pandemics; and (3) major industrial accidents or technological disasters. Many of the relevant capabilities would also be suitable for deployment in humanitarian crises.

Area 4.1: Demonstration projects

No demonstration projects foreseen in this activity for Security Research Call 1. See also chapter IV *Indicative priorities for future calls*.

Area 4.2: Integration projects

Expected impact: *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

The Security Research Call 1 calls for the following actions:

Topic SEC-2007-4.2-01 Network enabled command and control system

Technical content / scope: Widespread networking has the potential to provide significantly improved access to timely and relevant information to all crisis managers and first responders and to assist in the production of a common operational picture. The task is therefore to develop an integrated portfolio of network enabled capabilities for effective command and

control of the emergency crisis management organisation. The system will cover national and international operating procedures; organisational structures; information acquisition and management; decision support; interoperable communications; flexibility in planning and execution of operations.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-4.2-02 Integrated specialist search and rescue system

Technical content / scope: The task is to develop an integrated system to improve the ability to locate, assess, and rescue injured and/or contaminated victims in a CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) or natural disaster environment. This will include the detection of buried people; the use of sensors (acoustics, radars, video streaming, etc.) to enhance situation awareness; on-site monitoring of damaged structures and the environment; basic service systems (e.g. power generation); the ability to transmit, receive, and display data from specialist centres (command and control); mobile and autonomous specialist rescue and extraction equipment; biotechnological and medical counter measures; rapid decontamination; temporary protection during rescue and shelter for vicitims; etc.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-4.2-03 Post incident basic service restoration system

Technical content / scope: The task is to create an integrated system to improve the ability to rapidly deploy and/or rectify basic services (energy, water/pumps, communication, medical facilities etc.) after an incident and repair infrastructure and lines of communication (for command and control), which will allow crisis intervention teams to restore 'normality' as soon as possible. This will include mobile, scalable micro power grids to provide emergency electric power for key installations and first responders including integrated distributed power with the capability to connect different power sources, hardened for operating in harsh crisis management environments.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-4.2-04 Wireless communication for EU crisis management

Technical content / scope: The task is to build upon recent efforts on the software defined radio (SDR) architecture standard shared at European level and based upon the software communications architecture (SCA) concepts. The work consists of specifying, designing and developing a security referential platform including high data rate waveforms (software defining the services, communication protocols, interfaces, algorithms, security features, spectrum use, etc. for SDR) for security applications. The objective is to improve seamless communication between European security organisations and to demonstrate interoperability by means of deploying the SDR concept, architecture, and common information security architecture and defining and validating a new proposal for a security waveform for EU crisis management operations by demonstrating the portability of this security waveform between different referential platforms.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Area 4.3: Capability projects

Expected impact: *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

The Security Research Call 1 calls for the following actions:

Function: Situation awareness & assessment (surveillance)

Topic SEC-2007-4.3-01 Developing a common operational picture between regional and national authorities, first responders etc.

Technical content / scope: Effective command and control needs the sharing of information, processes, intervention methodologies and actions for integrated response services. In order to facilitate the development of a common operational picture between authorities, nations, first responders etc., the task is to develop novel technical support tools and mechanisms to collect, gather and disseminate information.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Command & control

Topic SEC-2007-4.3-02 Intelligent decision support

Technical content / scope: In order to enhance the efficiency of command and control by intelligent decision support systems, the task is to develop appropriate novel approaches to computer assisted decision making. Applications should be robust and facilitate the co-operation of operational units across organisational boundaries.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Function: Incident response

Topic SEC-2007-4.3-03 Personal equipment

Technical content / scope: The task is to develop novel personal equipment e.g. for first responders, providing effective protection (e.g. integrated in normal clothing) as well as operational and positional information. Systems should be mobile, lightweight, robust, easy to

use for heterogeneous teams and upgradeable with new developments (e.g. augmented reality systems integrated in smart suits). Research will involve domains such as smart clothes and equipments, decontamination techniques, biological technologies for biological and medical countermeasures, human survivability, protection and stress effects etc. Also see topic ICT-*SEC-2007-1.0.04 ICT support for first responders in crises occurring in critical infrastructures* with a view to compatibility.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Topic SEC-2007-4.3-04 Neutralisation of devices/effects

Technical content / scope: In order to contain and limit the effects of terrorist devices - including CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) and firearms - on the environment, the task is to develop novel, fast, wide range, mobile and easy to use approaches to the neutralisation of devices and effects, including techniques and systems for isolation, shielding, decontamination, etc.
Call: Security Research Call 1
Funding scheme(s): Collaborative project.

Activity 5: Improving *Security systems integration, interconnectivity and interoperability*

This activity is **not open** for self-standing actions in the Security Research Call 1. 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.

The Joint Call ICT & Security 1 **is open** for self-standing actions dealing with system integration, interconnectivity and interoperability issues *related to the security of infrastructures and utilities, in particular in the domain of energy and transport.*

<u>Activity 6: Security and society</u>

Technology is an important tool in preventing, responding, managing and mitigating potential security threats to European societies, but it is only part of the effective response. It must be applied in balanced combination with organisational processes and human intervention, which all determine each other and must be addressed by the actions. Cultural background plays an essential role, and also in balancing security as a societal value against other values. Thus research into political, social and human issues is required to complement the technology oriented research. When human beings are involved (as users), gender differences may exist. These must be addressed as an integral part of the research to ensure the highest level of scientific quality. Appropriate dissemination strategies should also make an integral part of the research. Many of the activities to be funded under this theme will make positive contributions to education and training and to raising general levels of awareness of the nature of the research undertaken and the benefits likely to accrue.

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*,

Expected impact: *Actions in this activity will provide improved insight and advice for security policy makers, security research programme makers and (mission oriented) security research performers. They do* not *generate general or specific knowledge about (in-)security, is reasons and consequences etc., but attain a broad and well-based understanding of the public administrative, cultural and societal framework 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.*

The Security Research Call 1 calls for the following actions:

Area 6.1: Citizens and Society

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 contribute to taking into account the human factor, people's behaviour, the interactions between citizens and authorities in security management or crisis situations and it will address 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-2007-6.1-01 Understanding factors that cause citizens' feeling of security and insecurity

Technical content / scope: In order to devise effective and long term security strategies and policies, a clear view as to how society perceives security and insecurity is required. The task is to study the factors which determine society's perception of security and/or insecurity and then to propose a method for implementation such that the results could guide and inform European and national policy formulation.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.1-02 Human behaviour before, during and after crisis situations to understand how people react to threat alerts and security instructions

Technical content / scope: The task is to carry out research into improving the understanding of people's behaviour in both crisis and 'steady-state' situations. The aim is to best tailor security related communication and instructions with a view to improving evacuation and protection activities. Actions will also address specific needs and appropriate timing with respect to people from differing faith, religious and cultural backgrounds from the survivors, casualties, deceased victims and bereaved families to workers, first responders and affected communities.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.1-03 Communication strategies of public authorities (including media strategies) before, during and after crises concerning risks, security threats and measures

Technical content / scope: In the case of crises, citizens are more likely to take coherent, correct and timely action if governments have the ability to communicate risk, threats and security measures in a focussed and optimised way. The task is to develop appropriate communication strategies in particular for public authorities and the media, taking into account all phases of a security incident and considering the influence of differing faith, religious and cultural backgrounds from the survivors, casualties, deceased victims and bereaved families to workers, first responders and affected communities.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Area 6.2: Understanding organisational structures and cultures of public users

An objective European joint security capability to handle security matters has to be based upon the resources and mandates of the Member States and Associated Countries. The distinct national systems must be interoperable, scaleable and allow for mobility where appropriate. Research under this area will regard the organisational structures, behavioural and cultural issues of end user organisations in order to ensure applicability, user friendliness and affordability of security technologies and solutions. It will also improve applicability concerning political accountability and democratic control aspects of public services within the security arena.

Topic SEC-2007-6.2-01 Behavioural, organisational and cultural issues to understand public user needs including those for joint European action

Technical content / scope: The tasks are (a) to assess the specific needs of private and public end users with a view to applicability, user friendliness and affordability of the results of the security research results of the 7th Framework Programme; (b) to carry out research into the organisational structures and distinct cultures of the numerous, complex and diverse public user organisations in order to successfully integrate them into research and development of security technologies; (c) analysing the consequences on the political, institutional, organisational and human elements underpinning technology based security policies and programs.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.2-02 Inventories of existing national resources, institutional mandates and practices across relevant sectors

Technical content / scope: The task is to address the need for general/operational interoperability, scalability and where appropriate mobility of the Member States' and Associated States' distinct national systems, in order to achieve an effective joint European capability to handle civil security issues. This will include in particular institutional design and issues concerning conflicting/complementary mandates and resources/best practices, in order to achieve better European connectivity between the existing national systems. The research should take into account behavioural, organisational and cultural issues that can have an impact on the effectiveness of public users, in particular linguistic barriers or stovepipe sectoral approaches.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Area 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 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-2007-6.3-01 Research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects)

Technical content / scope: The tasks are (a) to use foresight methods to address novel threats and technological opportunities and also emerging security related ethical, cultural and organisational challenges; (b) to apply scenario building techniques for systemic risk analysis as well as to inspire public debate and to foster shared understanding and self-organisation among stakeholders; (c) to address security as an evolving concept with a view to integrating diverse strands of research work and results in order to guide, orientate and structure future security related research activities.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.3-02 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)

Technical content / scope: 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 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Area 6.4: Security Economics

Security economics is the analysis of aggregate risks facing society and economy using rigorous analytical and empirical tools of economics, which should be regarded in particular with reference to the Lisbon agenda. 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-2007-6.4-01 Research survey on the emerging field of European security economics research to provide an analytical framework for complementary research

Technical content / scope: The task is to study (a) the fields to be covered under "European security economics", (b) ongoing research activities and open issues as well as (c) the relevant European players active in these fields in order to build up a European capacity for economic analysis and for policy making and with a view to establishing a security economics network. This might include topics such as indicators for the level of factual security as well as the security related impact of political measures, financial indicators relevant for security, effects of (in)security on individuals, firms and transaction costs between sectors of the economy, approaches to policy evaluation with respect to security issues (e.g. using natural or social experiments to isolate the effects of interventions).
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at coordinating and supporting research activities).

Topic SEC-2007-6.4-02 European Security Indicator: methodological research to provide a few select indicators of security and security policy in Europe measuring the effects of both insecurity and security policies on the economy

Technical content / scope:
The task is to develop a set of indicators that together could serve as 'European Security Indicator'. Both the level of factual security as well as the security related impact of political measures should be addressed, with a view to achieving an objective reference instead of relying on (in)security as perceived by public opinion. This will include an assessment of the economic implications of both insecurity and of the implementation of security policies. It will also assess potential changes in market structures that might be initiated by regulatory measures which aim at stimulating "secure growth" and thus stimulate industries to provide security-enhancing products or services. Eventually it will take into account changes in criminality and assess crime risks.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.4-03 Public finance: Studying the scale, function and roles of various types of government security spending across Europe and time.

Technical content / scope: The task is to develop econometric models that together provide an insight into the scale, scope and direction of public investments in security. Such scaleable models, capable of accommodating national as well as European perspectives, should combine the outcomes of various forms of threat and gap analysis to establish the historical effectiveness of public investments in security and provide guidance as to improving both the efficiency and effectiveness of future investments.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

<u>Area 6.5: Ethics and justice</u>

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 and legal questions based on divergent ethical, religious, historical and philosophical backgrounds. Aspects of social exclusion leading to the formation of areas of insecurity within Europe may also be considered (e.g. suburbs, poverty stricken inner cities) as well as of the European Neighbourhood Policy" that are 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-2007-6.5-01 How to take the necessary measures to ensure the security of citizens while respecting the civic rights and how this is implemented in practice, particularly addressing the issue of privacy and security

Technical content / scope: The task is to establish a network to analyse the wider context of government security policies and responses to security threats, e.g. in counter-terrorism, in particular from the point of view of personal data protection and integrity of information or of the limits and conditions for any potential loss of privacy or infringement of liberty; in particular also addressing the acceptability of security related technologies.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-6.5-02 Ethical implications of the continuum of internal and external security

Technical content / scope: The distinction between internal and external security is increasingly blurred. Internal security technologies and polices have a direct effect both on communities within the EU and also on the EU's neighbouring countries. The task is to examine the effects in terms of scale, scope and depth and to put forward possible remedial solutions as an aid to decision makers.
Call: Security Research Call 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Activity 7: Security Research coordination and structuring

The Security theme, aiming at contributing to increased security for Europe's citizens whilst 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. And 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.

Expected impact: *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.*

The Security Research Call 1 calls for the following actions:

Topic SEC-2007-7.0-01 Technology Watch

Technical content / scope: In order to ensure effectiveness and efficiency of the Security theme and the consequent need to be complementary to relevant actions carried out elsewhere, and with a view to ensuring the awareness of underpinning technologies that could be 'spun-in' to civil security applications, the task is to perform a 'European Technology Watch'. This should consist of (a) a web based IT system that acts as both a repository for data (technology watch list) and an interface for interrogating the data to user requirements, (b) a network of contact points responsible for managing data entries as well as an independent "neutral" lead coordinator, and (c) a panel to monitor its implementation and advise the EC, Member States and Associated Countries and EU security research community on emerging technologies. The Technology Watch should be based on a joint capability and technology taxonomy, and it needs to take into account and if possible build upon relevant ongoing initiatives.
Call: Security Research Call 1
Funding scheme(s): Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-7.0-02 European Security Research Networks (incl. for standardisation)

Technical content / scope: With a view to informing the Security theme as well as security research initiatives in the Member States and Associated Countries, and also to exploit opportunities outside the Community scope, the task is to establish European networks of Member States and Associated Countries, private sector security research requirement owners, operative end-users and technology supply chain experts. This will facilitate a common understanding of needs amongst research requirement owners and end-users, with the support of technology experts, so as to identify technology solutions to meet the needs (on the basis of a joint capability and technology taxonomy), and thus will ensure increased effectiveness and efficiency. Technology oriented research strategies should be complemented by society related research strategies.
Strategic R&T roadmaps should be proposed to guide, orientate and underpin European, national and private research programmes. The networks should furthermore identify possible joint programmes or projects which could be undertaken between services, Member States / Associated Countries and EC or international organisations. Eventually, the networks should address how to cooperate effectively amongst user and supply side stakeholders to deliver security capabilities, how to encourage security innovation, and how to strengthen the technology supply chains from primary research via development to procurement. They should also contribute to the definition of new standards.
Preferably the networks should be based on existing organisations and structures (e.g. the CEN for standardisation). A steering group should ensure coherence between, and across, the different stakeholders and activities. Activities could be structured by mission to achieve homogeneous networks of users and experts. Where appropriate, they should be inter-sectoral but must have a common basis of needs and possible solutions. Within strict conditions of confidentiality, maximum use should be made of secure ICT platforms and networks to exchange relevant data.
The activities of the networks could include an advisory function to the network of Member States' / Associated Countries' security research contact points established under topic SEC-2007-7.0-04.
Call: Security Research Call 1
Funding scheme(s): Coordination and support action (aiming at coordinating research activities).

Topic SEC-2007-7.0-03 Network of facilities for testing, evaluating and certifying security related products

Technical content / scope: With a view to meeting the objectives of the Security theme, the task is to facilitate the implementation of novel security technologies, products and services (this also includes other types of products and services which should become more 'crime-proof'). These need to be validated to meet specific standards and to be interoperable with other, including existing, systems. Thus the task is to establish a network of facilities for testing, evaluating and certifying security related products and services to contribute to the further development and improvement of security standards and to quantifiable targets for security levels in security policies. This will help the creation and extension of a European market for security products and services. Activities of the European Committee for Standardization (CEN)[18] need to be taken into account.

---

[18] *CEN Technical Board/Working Group 161: Protection and Security of the Citizen*

Call: Security Research Call 1
Funding scheme(s): Coordination and support action (aiming at coordinating research activities).

Topic SEC-2007-7.0-04 Transparency and networking amongst Member States and Associated Countries

Technical content / scope: 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 establish a Member States' and Associated countries' network of competent and politically relevant national and where appropriate regional contact points that will (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); (c) explore and demonstrate coordinated and/or joint initiatives in these core areas. The action will be similar to the principles of ERA-NET. This topic is open for full scale ERA-NET proposals as well, which should be submitted under this call[19].
Call: Security Research Call 1
Funding scheme(s): Coordination and support action.

Topic SEC-2007-7.0-05 Supply chains and market integration

Technical content / scope: With a view to involving the best intellectual and technological capabilities available throughout Europe in the security technology supply chains, including the yet untapped potential, the task is to identify opportunities and weak spots in the supply chains, to identify appropriate organisations (in particular SMEs) not yet involved or settled in the security (research) domain, to help them understand security related targets, mechanisms and opportunities and to facilitate their access to the main stakeholders and integrators of these technology supply chains. The action needs to take into account and if possible build upon relevant ongoing initiatives.
Call: Security Research Call 1
Funding scheme(s): Coordination and support action (aiming at supporting research activities).

Topic SEC-2007-7.0-06 Trans-national co-operation among NCPs

Technical content / scope: The task is to reinforce the network of National Contact Points (NCP) for the 7th Framework Programme under the Security theme, by promoting trans-national co-operation. The action will focus on identifying and sharing good practices. This may entail various mechanisms such as benchmarking, joint workshops, training, and twinning schemes. Practical initiatives to benefit cross-border audiences may also be included, such as trans-national brokerage events. The specific approach should be adapted to the nature of the theme, to other relevant ongoing actions and to the capacities and priorities

---

[19] *Not the joint call for ERA-NETs across the Themes- See Annex IV*

of the NCPs concerned. Special attention will be given to helping less experienced NCPs rapidly acquire the know-how accumulated in other countries.

Proposals are expected to include all NCPs who have been officially appointed by the relevant national authorities. Other participants from the EU and associated countries are ineligible. If certain NCPs wish to abstain from participating, this fact should be explicitly documented in the proposal. The Commission expects to receive a single proposal under this heading.

Call: Security Research Call 1

Funding scheme(s): Coordination and support action (aiming at coordinating research activities); indicative budget: up to 3 M€. It is expected that the project should last for a maximum of 5 years, and should in any case finish before March 2013.

Expected impact: *An improved NCP service across Europe, therefore helping simplify access to calls of the 7th Framework Programme, 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.*

II.2 Joint Call ICT & Security 1 (FP7-ICT-SEC-2007-1)

The activity open in this call corresponds
- For the ICT Theme[20], to Objective *3.1.2.2: Critical Infrastructure Protection;*
- For the Security Theme, to Activity 5 *Improving security systems integration, interconnectivity and interoperability* of the *Security Research Call 1*.

Activity 1: Security systems integration, interconnectivity and interoperability

For each of the four mission areas, integration, connectivity and interoperability play a very specific enabling role - both within and amongst missions. The purpose of this section is to draw attention to, and in some instances expand upon, those common issues of importance mentioned within the mission areas. Activities will *enable* and/or *contribute to the performance* of technology required for building up the necessary capabilities, thus focusing on cross-cutting issues such as: enhancing the interoperability and intercommunication of systems, equipment, services and processes while ensuring their reliability, protection of confidentiality and integrity of information, traceability of all transactions and their processing etc. Activities will also address standardisation and training matters (including such with respect to cultural, human and organisational interoperability).

To reach these objectives, a joint call with the ICT Theme is organised as follows:

Joint Call between the ICT Theme and the Security Theme on Critical Infrastructure Protection

The interoperability and interconnectivity of supply systems is one of the cornerstones of the functioning of our societies. The vulnerabilities in the intercommunication of systems, equipment, services and processes and their resilience against malicious attacks of terrorism and (organised) crime are elementary to the security of the citizens.

The objective of the joint call is to make key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare, or transportation systems more secure and dependable. The aim is to protect such critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.

The joint call is structured around two specific foci.

---

[20] *For more details concerning these topics consult the ICT Work programme.*

Focus of the ICT Theme

Objective ICT-SEC-2007.1.7

The <u>first focus</u> is called for by the *ICT* theme[21] and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures so that they survive malicious attacks or accidental failures, guarantee integrity of data and continuous provision of responsive and trustworthy services, and support dynamically varying trust requirements. This includes:

a) Understanding and managing the interactions and complexity of interdependent critical infrastructures; mastering their vulnerabilities; preventing against cascading effects; providing recovery and continuity in critical scenarios (including research towards designing and building self adapted and self healing complex systems); and security and dependability metrics and assurance methods for quantifying infrastructure interdependencies.

b) Designing and developing secure and resilient networked and distributed information and process control systems; systemic risk analysis and security configuration and management of critical information infrastructures and dynamic assurance frameworks for interconnecting them with critical infrastructures; availability of security forensics.

c) Developing longer term visions and research roadmaps; metrics and benchmarks for comparative evaluation in support of certification and standardisation; international cooperation and co-ordination with developed countries; coordination with related national or regional programmes or initiatives.

Call: Joint Call ICT & Security 1

Funding schemes: (a) and (b) Collaborative Projects ('small or medium scale focused research projects' only); (c) Coordination and support actions (aiming at coordinating or at supporting research activities).

Focus of the Security Theme

The <u>second focus</u> is called for by the Security theme and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available transport and energy infrastructures that survive malicious attacks or accidental failures and guaranteeing continuous provision of services. The following topics are called:

Topic ICT-SEC-2007-1.0-01 Risk assessment and contingency planning for interconnected transport or energy networks

Technical content / scope: The task is to develop integrated frameworks and agreed, common methodologies for (a) global analyses and assessment of risks, failures and vulnerabilities of transport or energy infrastructures, and (b) management and contingency

---

[21] *For more details concerning these topics consult the ICT Work Programme.*

planning based on the compilation and analyses of emergency plans, to assure interoperability between interconnected and interdependent heterogeneous transport or energy infrastructures.
Call: Joint Call ICT & Security 1
Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic ICT-SEC-2007-1.0-02 Modelling and simulation for training

Technical content / scope: Security crises concerning cross-border interconnected European transport or energy infrastructures can lead to effects with high impacts of disruption. The task consists of modelling & simulation including scenario building for handling security incidents to support the training of crisis managers.[22]
Call: Joint Call ICT & Security 1
Funding scheme(s): Collaborative project.

Topic ICT-SEC-2007-1.0-03 Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures

Technical content / scope: The task consists of developing tools that integrate smart surveillance information from interconnected and heterogeneous transport or energy infrastructures in order to build up high level situation awareness. The objective is to enable optimized decision making required for cross-border interoperable crisis management to ensure secure, resilient and always available transport or energy infrastructures.[23]
Call: Joint Call ICT & Security 1
Funding scheme(s): Collaborative project.

Topic ICT-SEC-2007-1.0-04 ICT support for first responders in crises occurring in critical infrastructures

Technical content / scope: The task consists of developing novel technologies for personal digital support systems as part of an integral, secure emergency management system to support first responders in crises occurring in various types of critical infrastructures under all circumstances. The action has to build upon ongoing research on emergency management, secure wireless communication, first responder technologies, etc. See as well topic *SEC-2007-4.3.03 Personal equipment* with a view to compatibility and complementarity.
Call: Joint Call ICT & Security 1
Funding scheme(s): Collaborative project.

Expected impact:
Actions in this area will provide significant improvement in the security, performance, dependability and resilience of complex and interdependent critical infrastructures while considering as well organisational dynamics, human factors, societal issues and related legal aspects.

---

[22] *See also COM(2005) 576 final. Green Paper on a European Programme for Critical Infrastructure Protection.*
[23] *Same as previous footnote.*

They will reinforce European industry's potential to create important market opportunities and establish leadership.

They will contribute to establishing, strengthening and preserving trust in the use of technologies for the protection of critical infrastructures. This includes creating sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding potential classification requirements, international co-operation needs, communication and implementation strategies etc.), in order to ensure acceptance of such technologies by relevant stakeholders.

They will achieve a more effective protection through enhanced co-operation, coordination and focus across Europe, and contribute to the development and promotion of metrics, standards, evaluation and certification methods and best practice in security of critical infrastructures.

Indicative budget for the Security Work Programme 2007-2008

More information will be provided on *http://cordis.europa.eu/fp7/calls/*.

Call/activity	ENTR Total[24] M€	ENTR 2007 M€	ENTR 2008[25] M€	INFSO 2008[26] M€
Call FP7-SEC-2007-1	156.5	80,3	76,2	
Call FP7-ICT-SEC-2007-1*	20	0	20	**20**
General Activities (cf. Annex 4)	5.6	5,6	0	
Other Activities: • Evaluations (0,8 M€) • Information / communication (0,2 M€)	1	1	0	
Estimated total budget allocation	183.1	**86,9**	**96,2**	

Summary of budget allocation to general activities for 2007 (cf. Annex 4)

Cordis	0,17 M€
Eureka / Research Organisations	0,02 M€
COST	0,74 M€
ERA-NET	0,24 M€
RSFF	4,43 M€
Total	**5,6 M€**

---

[24] The total funding is shown, together with the breakdown of how this is financed through the annual budgets.

[25] Under the condition that the preliminary draft budget for 2008 is adopted without modifications by the budgetary authority

[26] Under the condition that the preliminary draft budget for 2008 is adopted without modifications by the budgetary authority

Indicative budget allocation for the Security Work Programme 2007

Security Research Call 1 (FP7-SEC-2007-1)

Up to an indicative 3% for international co-operation.

Up to an indicative 2% for ERA-NET.

An indicative 58% (deviation possible from 50% to 70%) for integration projects (Areas 1.2, 2.2, 3.2, 4.2).

An indicative 35% (deviation possible from 25% to 45%) for capability projects (Areas 1.3, 2.3, 3.3, 4.3, in activity 6).

An indicative 7% (deviation possible from 4% to 12%) for topics which are implemented through coordination and supporting activities (Areas 1.1, 2.1, 3.1, 4.1, in activity 6, activity 7).

Joint Call ICT & Security 1 (FP7-ICT-SEC-2007-1)

Up to an indicative 3% for international co-operation.

An indicative 90% (deviation possible from 80% to 100%) for collaborative projects.

Up to an indicative 10% for coordination and support actions.

III   IMPLEMENTATION OF CALLS

III.1 Security Research Call 1 (FP7-SEC-2007-1)

- Call title: Security Research Call 1

- Call identifier: FP7-SEC-2007-1

- Date of publication: 22 December 2006

- Deadline: 31 May 2007, at 17.00 h Brussels local time

- Revised indicative budget[27]: 156,5 M€

- Topics called:

ACTIVITY/ AREA	TOPICS CALLED	FUNDING SCHEMES
1. Security of citizens / *1.2 Integration projects*	*SEC-2007-1.2-01 Intelligent urban environment observation system*	*Collaborative project*
	SEC-2007-1.2-02 Integrated mobile security kit	
1. Security of citizens / *1.3 Capability projects*	*SEC-2007-1.3-01 Stand off scanning and detection of hidden dangerous materials and/or stowaways, fast and reliable alerting and specification*	*Collaborative project*
	SEC-2007-1.3-02 Improved control of explosives throughout their "lifecycle"	
	SEC-2007-1.3-03 Localisation and tracking of components of substance production	
	SEC-2007-1.3-04 Observation through water, metal, ground etc	
	SEC-2007-1.3-05 Water distribution surveillance	
	SEC-2007-1.3-06 Secure strategic information management system	
2. Security of infrastructures and utilities / 2.1 Demonstration projects	*SEC-2007-2.1-01 Security of critical infrastructures related to mass transportation*	*Coordination and support action (supporting)*
2. Security of infrastructures and utilities / 2.2 Integration projects	*SEC-2007-2.2-01 Integrated protection of rail transportation*	*Collaborative project*
2. Security of infrastructures and utilities / 2.3 Capability projects	*SEC-2007-2.3-01 Detection of unattended goods and of owner*	*Collaborative project*
	SEC-2007-2.3-02 Detection of abnormal behaviour of vehicles &	

---

[27] *This amount includes 76,2M€ from the 2008 budget, which is added under the condition that the preliminary draft budget for 2008 is adopted without modifications by the budget authority.*

	threats, both in wide and small land areas	
	SEC-2007-2.3-03 Detection of abnormal behaviour	
	SEC-2007-2.3-04 Small area 24 hours surveillance	
***3. Intelligent surveillance and border security** / 3.1 Demonstration projects*	*SEC-2007-3.1-01 Integrated border management system*	*Coordination and support action (supporting)*
***3. Intelligent surveillance and border security** / 3.2 Integration projects*	*SEC-2007-3.2-01 Main port security system (including containers)*	*Collaborative project*
	SEC-2007-3.2-02 Unregulated land borders surveillance system	
	SEC-2007-3.2-03 Integrated check points security	
***3. Intelligent surveillance and border security** / 3.3 Capability projects*	*SEC-2007-3.3-01 Air 3D detection of manned and unmanned platforms*	*Collaborative project*
	SEC-2007-3.3-02 Surveillance in wide maritime areas through active and passive means	
	SEC-2007-3.3-03 Solutions for ensuring end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems	
***4. Restoring security and safety in case of crisis** / 4.2 Integration projects*	*SEC-2007-4.2-01 Network enabled command and control systems*	*Collaborative project*
	SEC-2007-4.2-02 Integrated specialist search and rescue system	
	SEC-2007-4.2-03 Post incident basic service restoration system	
	SEC-2007-4.2-04 Wireless communication for EU crisis management	
***4. Restoring security and safety in case of crisis** / 4.3 Capability projects*	*SEC-2007-4.3-01 Developing a common operational picture between regional and national authorities, first responders etc.*	*Collaborative project*
	SEC-2007-4.3-02 Intelligent decision support	
	SEC-2007-4.3-03 Personal equipment	
	SEC-2007-4.3-04 Neutralisation of devices/effects	
***6. Security and Society** / 6.1 Citizens and Society*	*SEC-2007-6.1-01 Understanding factors that cause citizens' feeling of security and insecurity*	*Collaborative project and Coordination and support action (supporting)*
	SEC-2007-6.1-02 Human behaviour before, during and after crisis situations to understand how people react to threat alerts and security instructions	
	SEC-2007-6.1-03 Communication strategies of public authorities (including media strategies) before, during and after crises concerning risks, security threats and measures	
***6. Security and Society** / 6.2 Understanding organisational structures and cultures of public users Society*	*SEC-2007-6.2-01 Behavioural, organisational and cultural issues to understand public user needs including those for joint European action*	*Collaborative project and Coordination and support action (supporting)*
	SEC-2007-6.2-02 Inventories of existing national resources, institutional mandates and practices across relevant sectors	

6. Security and Society / 6.3 Foresight, scenarios and security as an evolving concept	*SEC-2007-6.3-01 Research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects)*	*Collaborative project and Coordination and support action (supporting)*
	SEC-2007-6.3-02 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)	
6. Security and Society / 6.4 Security Economics	*SEC-2007-6.4-01 Research survey on the emerging field of European security economics research to provide an analytical framework for complementary research*	*Collaborative project and Coordination and support action (coordinating and supporting)*
	SEC-2007-6.4-02 European Security Indicator: methodological research to provide a few select indicators of security and security policy in Europe measuring the effects of both insecurity and security policies on the economy	*Collaborative project and Coordination and support action (supporting)*
	SEC-2007-6.4-03 Public finance: Studying the scale, function and roles of various types of government security spending across Europe and time.	
6. Security and Society / 6.5 Ethics and justice	*SEC-2007-6.5-01 How to take the necessary measures to ensure the security of citizens while respecting the civic rights and how this is implemented in practice, particularly addressing the issue of privacy and security*	*Collaborative project and Coordination and support action (supporting)*
	SEC-2007-6.5-02 Ethical implications of the continuum of internal and external security	
7. Security Research coordination and structuring	*SEC-2007-7.0-01 Technology Watch*	*Coordination and support action (supporting)*
	SEC-2007-7.0-02 European Security Research Network (incl. for standardisation)	*Coordination and support action (coordinating)*
	SEC-2007-7.0-03 Network of facilities for test and validation of security related products	
	SEC-2007-7.0-04 Transparency and networking amongst Member States and Associated Countries	
	SEC-2007-7.0-05 Supply chains and market integration	*Coordination and support action (supporting)*
	SEC-2007-7.0-06 Trans-national co-operation among NCPs	*Coordination and support action (coordinating)*

- **Evaluation procedure**:

  A one-stage submission procedure will be followed.

  Proposals will be evaluated in a single-step procedure.

- **Indicative evaluation and contractual timetable**: Evaluations of proposals are expected to be carried out in June/July 2007. It is expected that the contract negotiations for the shortlisted proposals will be open from September 2007 to July 2008.

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

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

  The minimum number of participating entities required, for all funding schemes, is set out in the Rules for Participation: For Collaborative projects, the minimum condition shall be the participation of 3 legal entities, each of which is established in a Member State or Associated Country and no two of which are established in the same Member State or Associated Country. For Coordination and Supporting Actions aiming at *supporting* research activities and policies the minimum condition shall be the participation of one legal entity. For Coordination and Supporting Actions aiming at *coordinating* research activities and policies the minimum condition shall be the participation of three legal entities, each of which is established in a Member State or Associated Country, and no two of which are established in the same Member State or Associated Country.

  Proposals must not contain any classified information, this will immediately lead to declaring them ineligible (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 *and provide evidence* of the clearance of all relevant persons and facilities. Consortia have to clarify issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal. Proposals need to provide a *security aspect letter,* indicating the levels of classification required. Appropriate arrangements have to be included in the consortium agreement.

  Proposers claiming that their proposal should receive Community funding up to 75% should demonstrate in the proposal that the required conditions (very limited market size and a risk of "market failure", the need for accelerated equipment development in response to new threats) apply. The final decision will be based on the recommendations of the relevant evaluation panel.

  Consortia are strongly encouraged to actively involve SMEs and end users. Their presence in the consortia will be judged under the evaluation criterion 'Quality and efficiency of the implementation and the management' with a view to meeting the main objectives of the theme.

  Proposers responding to SEC-2007-7.0-06 must be NCPs officially appointed by the relevant national authorities, all others will be considered non eligible.

  The evaluation panel will comprise end users as well.

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.

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.

Coordinators of all integration project proposals and of all demonstration project (phase 1) proposals that pass all the evaluation thresholds can 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.

The forms of grants which will be offered are specified in Annex 3 to the Co-operation work programme

III.2 Joint Call ICT & Security 1 (FP7-ICT-SEC-2007-1)

- Call title: Joint Call ICT & Security 1

- Call identifier: FP7-ICT-SEC-2007-1

- Date of publication [28]: 30 August 2007

- Deadline[29]: 29 November 2007, at 17.00 h Brussels local time

Indicative budget: The indicative call budget is foreseen to be 40 M€, provided by the Security theme (20 M€)[30] for actions addressing the specific focus 2 and by the ICT theme (20 M€)[31] for actions addressing the specific focus 1. Out of the Security theme's budget (20 M€), an indicative 1 M€ is available for international co-operation.

- Topics called:

ACTIVITY/ AREA ICT THEME	TOPICS CALLED	FUNDING SCHEMES
Focus 1. Pervasive and Trusted Network and Service Infrastructures / Critical Infrastructure Protection	*ICT-SEC-2007.1.7 Technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures**	*Collaborative project and Coordination and support action (coordinating, supporting)*

ACTIVITY/ AREA SECURITY THEME	TOPICS CALLED	FUNDING SCHEMES
Focus 2. Security systems integration, inter-connectivity and interoperability	*ICT-SEC-2007-1.0-01 Risk Assessment and contingency planning for interconnected transport or energy networks*	*Collaborative project and Coordination and support action (supporting)*
	ICT-SEC-2007-1.0-02 Modelling and simulation for training	*Collaborative project*
	ICT-SEC-2007-1.0-03 Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures	
	Topic ICT-SEC-2007-1.0-04 ICT support for first responders	

---

[28] *The Director-general responsible for the call may publish it up to one month prior to or after the envisaged date of publication*

[29] *At the time of the publication of the call, the Director-general responsible may delay this deadline by up to two months.*

[30] *An amount of 20 M€ is given by the Security theme from the 2008 budget, under the condition that the preliminary draft budget for 2008 is adopted without modifications by the budget authority.*

[31] *An amount of 20 M€ is given by the ICT theme from the 2008 budget, under the condition that the preliminary draft budget for 2008 is adopted without modifications by the budget authority.*

	in crises occurring in critical infrastructures	

- **Evaluation procedure:**

  A one-stage submission procedure will be followed.

  Proposals will be evaluated in a single-step procedure.

- **Indicative evaluation and contractual timetable**: Evaluations of proposals are expected to be carried out during the month of January 2008. It is expected that the contract negotiations for the shortlisted proposals will be open from March to July 2008.

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

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

  The minimum number of participating entities required, for all funding schemes, is set out in the Rules for Participation: For Collaborative projects, the minimum condition shall be the participation of 3 legal entities, each of which is established in a Member State or Associated Country and no two of which are established in the same Member State or Associated Country. For Coordination and Supporting Actions aiming at *supporting* research activities and policies the minimum condition shall be the participation of one legal entity. For Coordination and Supporting Actions aiming at *coordinating* research activities and policies the minimum condition shall be the participation of three legal entities, each of which is established in a Member State or Associated Country, and no two of which are established in the same Member State or Associated Country.

  Proposers should indicate in which of the two specific foci of the call their proposal best fits. There will be a joint evaluation of proposals submitted under the two specific foci. During the evaluation, evaluators could move, in a transparent manner, proposals from one specific focus to the other, if they consider that a proposal would fit better there and that this would be to the benefit of the proposers.

  Proposals must not contain any classified information, this will immediately lead to declaring them ineligible (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 *and provide evidence* of the clearance of all relevant persons and facilities. Consortia have to clarify issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal. Proposals need to provide a *security aspect letter,* indicating the levels of classification required. Appropriate arrangements have to be included in the consortium agreement.

  Proposers addressing topics of the specific focus 2 and claiming that their proposal should receive Community funding up to 75% should demonstrate in the proposal that the required conditions (very limited market size and a risk of "market failure", the need for accelerated equipment development in response to new threats) apply. The final decision will be based on the recommendations of the relevant evaluation panel.

  Consortia are strongly encouraged to actively involve SMEs and end users. Their presence in the consortia will be judged under the evaluation criterion 'Quality and efficiency of the implementation and the management' with a view to meeting the main objectives of the theme.

  The evaluation panel will comprise end users as well.

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.

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.

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.

The forms of grants which will be offered are specified in Annex 3 to the Cooperation work programme

IV INDICATIVE PRIORITIES FOR FUTURE CALLS

Indicative roadmap of future calls

12/2006:	Security Research Call 1
08/2007:	Joint Call ICT & Security 1
06/2008:	Security Research Call 2
06/2009:	Security Research Call 3
09/2009	*Optional Call (for Demonstration projects phases 2)*
06/2010:	Security Research Call 4
09/2010	*Optional Call (for Demonstration projects phases 2)*
06/2011:	Security Research Call 5
06/2012:	Security Research Call 6

Indicative approach of future calls

- **Security Research Call 2** will be open for the *first phases* of two to three more demonstration projects and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

  The demonstration projects (phase 1 only) called for will be

  in Activity 1: Security of citizens
    o *Logistic and supply chain security*
    o *CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives)*

  in Activity 4: Restoring security and safety in case of crisis
    o *Aftermath crisis management system*

  The integration projects called for will be those called for but not sufficiently covered by the first call, as well as:

  in Activity 1: Security of citizens
    o *Advanced forensic toolbox*
    o *Secure strategic information management system*

  in Activity 2: Security of infrastructures and utilities
    o *Detection system for abnormal behaviour*
    o *Open space security*
    o *Built infrastructure protection*

  in Activity 3: Intelligent surveillance and border security
    o *Sea borders surveillance system*
    o *Extended smart borders*

  in Activity 4: Restoring security and safety in case of crisis
    o *First responder of the future*

For more information on these demonstration and integration project topics, the ESRAB report can be consulted.

The <u>capability projects</u> called for will be selected from those not yet sufficiently covered by the first call, as well as those recommended by ESRAB but not included in the first call.

- **Security Research Call 3** will be open for the *second phases* of the demonstration projects* called for in Security Research Call 1 and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

- **Security Research Call 4** will be open for the *second phases* of the demonstration projects* 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.

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

- **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.

On the level of the <u>capability projects</u>, future calls will invite actions along the following functions, which group the capabilities as required in all security missions:

Function A: Risk assessment, modelling & impact reduction
Function B: Doctrine & operation
Function C: Training & exercises
Function D: Detection, identification & authentication
Function E: Positioning & localisation
Function F: Situation awareness & assessment (surveillance)
Function G: Information management
Function H: Intervention & neutralisation
Function I: Communication
Function J: Command & control
Function K: Incident response