*** Please note that this document ***

- only has a draft status (do not communicate with the European Commission about the content)

- is confidential (only share selected paragraphs of the text and not the whole document)

Secure societies challenge

This Work Programme will contribute to the implementation of the policy goals of the Europe 2020 strategy, the Security Industrial Policy[1], the Internal Security Strategy[2] and the Cyber Security Strategy[3].

This Work Programme is about protecting our citizens, society and economy as well as our assets, infrastructures and services, our prosperity, political stability and well-being. Any malfunction or disruption, intentional or accidental, can have detrimental impact with high associated economic or societal costs.

The primary aim of this Work Programme is thus to fight crime and terrorism ranging from new forensic tools to protection against explosives (call 1); to enhance the resilience of our society against natural and man-made disasters, ranging from new crisis management tools to communication interoperability, and to develop novel solutions for the protection of critical infrastructure (call 2); to improve border security, ranging from improved maritime border protection to supply chain security (call 3); and to provide enhanced cybersecurity (call 4), ranging from secure information sharing to new assurance models.

European citizens, businesses and administrations are increasingly dependent on Information and Communication Technologies (ICTs) for their daily activities. ICTs boost productivity, innovation, commercial exchanges and societal changes. Hence, the actual or perceived lack of security of digital technologies is putting at risk the European economy and society. Moreover, criminal actors have now widely embraced the new technologies to perpetrate crime. Therefore, in the EU and worldwide cybersecurity, has become a political and economic priority. It is, thus only natural that cyber security has become part of the Secure Societies Challenge.

We thus see a convergence of traditional security needs and the digital world. Whilst many infrastructures and services are privately owned and operated, protection of public safety and security are the responsibility of the public authorities. Therefore security is an issue that can only be tackled effectively if all stakeholders cooperate.

In consequence this Work Programme addresses both private companies/industry and institutional stakeholders. Calls 1 to 3 of the Work Programme are tightly specified as they respond to a well identified need by the end-users, be it law enforcement agencies, border guards or first responders. They are to respond to actual shortcomings in tools and methods to provide security. Call 4 of the Work Programme is more forward looking, proposing to make use of the next, as yet untrialled at large scale, ICT technology to propose innovative solutions to security risks. The expected outcomes will result in a faster transposition of the research results into commercial products or applications, and some could then become the take-up measures of Calls 1 to 3. Therefore the latter objective is defined in broader terms, allowing for a wider differentiation of concepts and stakeholders.

This difference is also reflected in the choice of different funding instruments. Calls 1 to 3 follow a building block structure (see figure 1) to contribute to the mission objectives. On the lowest level of the building block structure, capability projects aim at building up and/or strengthening security

[1] COM(2012)417 final

[2] COM(2010) 673 final

[3] JOIN(2013)1 final

capabilities. 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. 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.In order to contribute to the mission objectives Call 4 makes use of the H2020 instruments to foster innovation, addressing close to market activities: the collaborative projects can either be 'demonstration/pilot' projects or 'first market replication' projects. .

Pre-commercial Procurement (PCP) differs from and complements the other building blocks, by involving directly – and supporting financially – end-user agencies (typically national or European authorities).

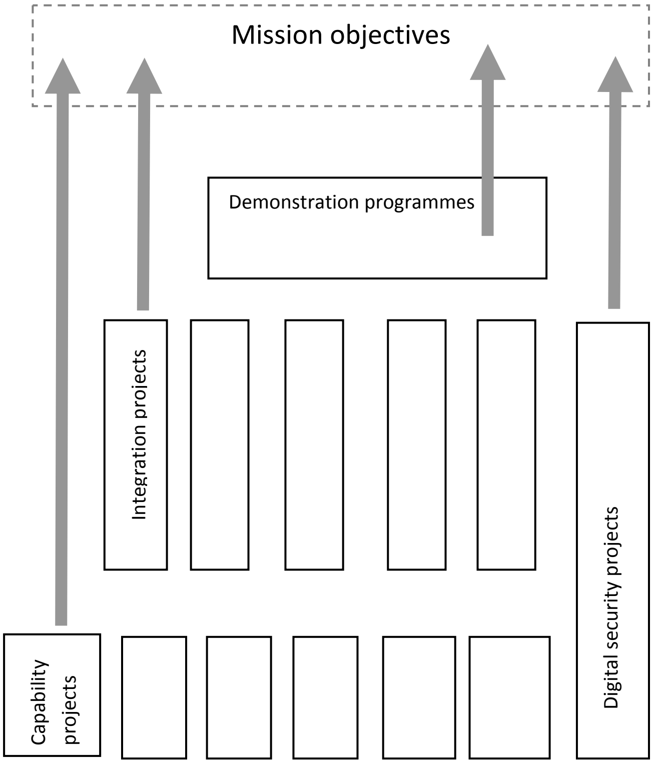

Figure 1: Research instruments to meet the Secure Societies' objectives

Overview of the calls:

Fight against crime and Terrorism

Contents

The ambition is both to avoid an incident and to mitigate its potential consequences. This requires new technologies and capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism), including understanding and tackling terrorist ideas and beliefs to also avoid aviation related threats.

This call is divided in four parts:

- Forensics
- Law enforcement capabilities
- Urban security
- Ethical/societal dimension

Forensics

1. Forensics topic 1: Tools and infrastructure for the fusion, exchange and analysis of big data for forensic investigation

Specific challenge:

The availability of petabytes of on-line and off-line information, both public and owned by the Law Enforcement Agencies (LEA), represents a valuable resource but also a management challenge. Access to huge amounts of data, structured (data-bases), unstructured (text), semi-structured (HTML, XML, etc.), available locally or over private LEA owned/shared networks or over the Internet, as well as additional heterogeneous data collected by LEA sensors such as Video, Audio and GPS, can easily result in an information overload and represent a problem instead of a useful asset. Research under this topic should aim to provide solutions at and beyond the state-of-the-art in the areas of intelligent use and management of complex and large amount of data for the discovery of correlated evidences to support forensic investigation on one hand and for the operational and situational awareness of law enforcement agencies on the other. The problem of extracting, integrating, exchanging and analysing large and complex data, as well as that of exploiting unstructured data (Natural Language Text, SMS) and adding intelligence (trends analysis, scenarios, etc.), has to be solved by means of at and beyond state-of-the-art technologies in the areas of Big Data, Data Analytics, Intelligent User's Interfaces, Information Retrieval, Weak Signal Analysis, Ontologies and Knowledge Representation.

Scope:

The effective management, exchange and analysis of such abundant, complex, heterogeneous, and international data while preserving privacy, security, and governance is a challenge for both forensic investigators and law enforcement agencies, the scope of this topic is two-fold.

Firstly, tools and platforms should be developed for sampling, analysing, evaluating, interpreting and recording forensic evidence from big data with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution. Applications should provide certainty with respect to the time and location of multimedia content and tests for authenticity and integrity of digital identities. Platforms should also provide users with semi-interactive techniques for understanding and visualizing data, including interdisciplinary approaches based on common, possibly standardized, ontologies and the exploitation of automated reasoning, information retrieval, and filtering tools. Human and organisational factors like multilingualism/multiculturalism as well as other trans-border issues (different terminologies, legislations, procedures) must be properly addressed.

Secondly, tools and platforms should be developed to enable LEAs to store, process, analyse, share, and exchange large amounts of heterogeneous data, including data arising from various types of sensors, with the aim of improving operational and situational awareness more efficiently. These should include applications which can provide early warning signs (e.g. predictions of future trends). Vendor locking has to be excluded. The development of a base line system for current and future end users should also envisaged and the software should follow Open Source concepts. This will enable transparency, and continuous maintenance and development after the end of the project. The software should provide fine-grained authorisation mechanisms to regulate data access. Support for logging and in general maintain the chain of custody is also required.

Proposals addressing both these areas should take previous research at European and national level into account. Methodologies, standards, expertise and procedures for training, simulation, and testing investigations to empower the experts and stream-line the processes involved in the fusion, exchange and analysis of big data for forensic investigation and operational/situational awareness for law enforcement purposes should be considered.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

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

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Improved capabilities for the LEA to conduct investigations with respect to privacy. Higher efficiency in accessing relevant data sources and retrieving information significant for forensic investigation. Improved capabilities for trans-border LEA data-exchange and collaboration.

Form of funding:
Collaborative Project 100% funding (Integration project)

Specific call year:
This topic is part of the call for 2015

2. Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime

Specific challenge:

Organised crime and criminals do not limit themselves to regional or national borders. Their crimes are thus leaving traces in multiple countries. Cross border access to evidence has become an absolute necessity for Law Enforcement Agencies (LEA) and judicial authorities.

Evidence gathering, collection and exchange at EU level should be usable from the field to the judge, independently of where the crimes have taken place. Rapid developments in technologies and communications in various fields go hand in hand with new opportunities for forensic science in order to keep the standards of forensic science in Europe at a high level level regarding juridical and technological questions..

Proposals for this topic should take into account the existing EU and national projects in this field.

Scope:

Proposals for this topic should focus on the development of EU-wide standards for the exchange of forensic data supporting evidence.

A platform integrating different techniques should be proposed in order to achieve better results for gathering evidence in the field of forensic research. Relying on knowledge-based fields such as artificial intelligence, machine learning, different procedures, tools and algorithm should be developed within this platform, based on the standard outlined above.

Where necessary new technologies should be developed for sampling, analysing evaluating, interpreting and recording forensic evidence with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.

Specific areas of research could be:

- Ballistic data, including gunshot residue.
- The establishment of a EU-wide database new synthetic drugs and precursors (detection protocols and analysis methodologies).
- Other types of pan-EU databases - like for instance soils etc.

In addition due to the variability and the wide range of crime types, procedures or methodologies should be developed or adapted to the specific crime features. Moreover, horizontal strategies could be proposed for profiling crimes or offenders and matching and predicting different type of crimes. This should lead to the establishment of a catalogue of these procedures or methodologies.

The involvement of existing EU wide forensics networks should be beneficial for the development of this proposal.

Where necessary new technologies should be developed for sampling, analysing evaluating, interpreting and recording forensic evidence with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The usage of the most advanced information technologies should allow improving and upgrading the current forensic systems in the European police institutions. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase. Moreover, it should contribute to a considerable improvement in the field of public security and improve trust of the citizen in the work of police forces in the EU.

Form of funding:
Collaborative Project 70% funding (Integration project)

Specific call year:
This topic is part of the call for 2015

3. Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRN materials

Specific challenge:

In the event of an accident or a terrorist attack (including those involving CBRN materials), the physical examination of the crime scene by hand may not be possible, or could be severly restricted due to the presence of hazardous material or risk of building collapse. Therefore, there is a need for the development of mobile, remotely- controlled technologies to enable an improved identification / detection of CBRN materials and collection of forensic material / evidence in a variety of situations and conditions.

Scope:

The objective of this project is to develop mobile, remotely controlled technologies to enable the assessment of hazardous scenes where the deployment of personnel is difficult as a result of an accident or terrorist attack. This should include technologies to enable the verification of CBRN materials through the identification / detection (including visual recognition) of the type of substance and the collection of forensic material / evidence. The output should be operational in a variety of weather and terrain conditions, and demonstrate they are cost effective. Proposals should link with existing projects.

Tools/technologies should have a minimal disruptive effect on the crime scene.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

An improved identification / detection and collection of forensic evidence in case of accidents or terrorist attacks involving CBRN materials will be of direct support to first responders, civil protection and public health services. In addition, dual-use applications will be considered with possible synergies being established with the European Defence Agency.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

4. Forensics topic 4: Internet Forensics to combat organized crime

Specific challenge:

The Internet is nowadays at the core of any business activity. All large and distributed organisations rely on the Internet for the exchange of data, information, and knowledge, both internally and externally, so as to organise and run their activities. Organized crime is no exception. The Internet has become an important tool for criminal organisations to carry out illegal activities. Research under this topic should refer to Internet Forensics as the set of investigation techniques concerned with Internet as a media used by organised crime in general - mainly to communicate and exchange data and information. A further and specific challenge is represented by the camouflage of the real nature of the concerned data and information. Due to the borderless nature of the Internet, specific trans-border aspects should be considered when dealing with Internet Forensics. Therefore, aside from the relevant technological aspects, legal and organisational issues like the co-ordination of different Law Enforcement Authorities (LEA) and the harmonisation of the different legal frameworks have to be addressed.

Scope:

Proposals should focus on how to extract, compare, correlate, filter and/or interpret suspect information, data, communications stored and/or transferred on the Internet obtained under a lawful warrant, in order to discover facts and evidence to support forensic investigations (including e.g. resolving identities in social networks, authorship identification on webfora etc.). Software and, if necessary, hardware tools, methods and guidelines should be proposed. They should tackle all the layers of analysis, from the data-packet level to the data mining, to language interpretation, semantic analysis, and information retrieval, including the multi-lingual aspects. Investigative techniques on any kind of crime using the Internet to some extent (to communicate, transfer data, etc.) should be concerned. The proposed solutions should enable accelerated searches of the huge amount of data-transfer that occurs on the Internet, and to discover and make clear (interpret) out of it the relevant data and information. At the same time, limited, or at least controlled, pervasiveness of the proposed solutions must be guaranteed, in order guarantee the privacy of all the internet users. Ethical issues have to be clearly addressed and appropriate solutions to fulfil the legitimate request of privacy by the citizens should be embedded in the very core of the proposed solutions.

Where necessary new technologies should be developed for sampling, analysing evaluating, interpreting and recording forensic evidence with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.The project will have to deal with the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Improved capabilities for the LEA to conduct investigations by using all information travelling and stored on the Internet. To enable an increase of the number of staff able to perform such kind of investigations. Increased crime prosecution capabilities.

Form of funding:
Collaborative Project 70% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

Law enforcement capabilities

5. Law enforcement capabilities topic 1: Develop novel monitoring systems and miniaturised sensors that improve Law Enforcement Agencies' evidence- gathering abilities

Specific challenge:

Investigations on the activities of criminal organizations (related with drugs or human trafficking, terrorism, or any other forms of organized crime) usually require Law Enforcement Agencies (LEAs) to use electronic equipment for legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way, while keeping for both the sensors part and the monitoring station all the legal, integrity and chain-of-custody requirements that will enable the presentation of evidences obtained this way at the Courts of Justice.

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

Scope:

The task is to develop a new type of sensors, monitoring station and their associated communication channel for LEA operation on the field according to their specification and subject to their validation at the end of the project taking into account the societal acceptance of the proposed solutions. Participation of LEAs in the definition of requirements and validation of results is essential, as only end-users are familiar with the challenges they frequently have to face in real operations within criminal investigations.

Proposals for this topic should ensure that the developed technologies must be such as to be upheld in Court.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

This action is directed to the substantial improvement of existing technologies and the development of new ones, and their direct and practical application to day-to-day needs that Law Enforcement Agencies are not able to realize efficiently with available commercial products including testing, validation and demonstration as justified.

Form of funding:
Collaborative Project 70% funding (Capability project)

Specific call year:
This topic is part of the call for 2014.

6. Law Enforcement capability 2: Detection and analysis of terrorist-generated content on the Internet

Specific challenge:

Due to the ease of publishing information on the Internet (Web site, blogs, social networks, newsgroups, etc.), terrorists increasingly exploit the Internet as a communication, intelligence, training, and propaganda tool where they can safely communicate with their affiliates, coordinate action plans, raise funds, and introduce new supporters into their networks. In order to cope with the dangers involved in the use of Internet by global terrorist organizations and grassroots terrorist cells, more efficient and effective automated techniques are required. Despite the often explicit or at least not disguised content of these web-sites, especially when used for propaganda, the huge amount of somehow related, yet not illegal, sites, represents a major obstacle to the reliable and fast analysis of their contents. Research should therefore develop and apply new and/or improved data and text mining methods to detect, categorize, analyse, and summarize terrorist-generated content. Aside this, modes of attacking, finding sources of threats, capturing and preserving data for forensic analysis, authenticating images and videos and conversely proving multimedia data falsification, should be investigated.

Scope:

Research should focus on the accurate identification of terrorist online communities (even hiding their real identity), accurate and fast categorization of malicious content published by terrorists and their supporters in multiple languages, large-scale temporal analysis of terrorism trends, and real-time summarization of multilingual information published by terrorists, including content filtering for mis- and disinformation and framing. In addition, linking pseudonyms and finding the original author should be part of the research.. The developed methodologies should be able to handle massive amounts of multilingual web content in minimal time.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

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

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

More effective prevention of terrorist activities planned and organized via the Internet through automated analysis of terrorist-generated content. Faster detection of grassroots terrorist cells from their online activitieş. Faster and more accurate detection and analysis of malicious content published by terrorists. Faster detection and analysis of terrorism trends. Reduction of the "information overload" on web intelligence experts due to automated summarization of the relevant content.

The usage of the most advanced information technologies will allow improving and upgrading the current mining systems in the European police/ intelligence agencies (the scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase). Moreover, it will contribute to a considerable improvement in the field of public security.

Form of funding:
Collaborative Project 70% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

7. Law enforcement capabilities topic 3: Securing the vehicle supply chain from production to destruction

Specific challenge:

In 21st century there is no need to get physically a car to receive the registration document, the number plate and to insure a high value vehicle. With this virtual registered and insured car, organized crime members can declare it as stolen. The direct benefits are the insurance payment of the car value and zero risk. International vehicle trafficking draws a yearly criminal benefit of approximately 5 billion Euro in Europe, increasing the risk of EU citizens to drive a stolen or defect car and impacting the legitimate vehicle business and the economy at large. International vehicle trafficking is one of the basics for organized crime groups to finance (illegal) operations worldwide.

Scope:

The main objectives are :

- To stop the criminal supply chain related to vehicles in Europe by enabling a comprehensive integration of information currently managed independently by all major stakeholders.
- To increase investigative capacities for police and custom authorities by significantly reducing the needed time to search for and assess essential information electronically.
- To strengthen public-private approach against vehicle crime in Europe and beyond through strong and structured cooperation between major stakeholders along the (criminal) supply chain.
- To enable strategic analyses for the purpose of targeted in concerned countries leading to crime prevention and crime detection.

The task is to create an e-platform where information could be exchanged between major stakeholders, with the following information available online to detect crime, avoid registration of stolen vehicles, avoid use of wrecks, ease police investigation:

- Manufactured Vehicle Identification Number (VIN) and country of export;
- VIN registered in each country;
- VIN insured and VIN declared 'wreck';
- VIN stolen.

The proposal should take into account existing European and national projects and includes representatives/stakeholders from all value chain (manufacturers, insurance companies, law enforcement agencies and international./European law enforcement organization, registration authorities, car dealers, etc.).

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

An effective and innovative tool in fighting crime and improving security should be developed. By stepping into state-of-the-art information management between public and private entities active in the fight against vehicle crime impacting EU citizen as well as EU business and law enforcement, the project is expected to bolster the prevention and detection of vehicle crimes.

Form of funding

Collaborative project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2014

8. Law enforcement capabilities topic 4: Trans-national cooperation among public end-users in security research stakeholders

Specific challenge:

The aim of the topic is to improve coordination at European level of various national or regional networks in different security research domains. Activities can concentrate on a specific core area or cover several areas. The focus of this challenge should be on the identification of the relevant technologies for law enforcement technologies.

Scope:

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

Expected impact:

It is expected to improve networking and coordination of various Member State activities relevant to security research at European level.

Form of funding

Coordination and Support Action 100% funding (Coordinating action)

Specific call year:
This topic is part of the call for 2014

Additional condition:

This topic is limited to public end-users, additionally proposals should contain at least 10 public authorities from 10 different Member States.

Urban security

9. Urban security topic 1: Innovative solutions to counter security challenges connected with large urban environment

Specific Challenge:

The current wave of urban growth, the largest in the world's history, is bringing various challenges and threats to urban security, especially in large urban environments. These challenges have also a strong impact on the security perception of the citizens and, by this, they can impact on the economic development and the quality of life.

Consequently, there is a growing need to go beyond the idea that only the law enforcement and criminal justice systems are tasked to tackle urban security challenges. On the contrary, new approaches and innovative solutions, including sustainable, affordable and transferrable security technologies, are needed to solicit citizens' engagement and direct participation in the improvement of the urban security conditions.

In this framework, and upon due consideration for the concerned ethical issues, recent technological advances and appropriate sensing mechanisms can help to make a city more transparent and readable as well as to empower the citizens in smart cities by ensuring that the main urban dynamics are unveiled and available to the public.

To this end, a bottom-up approach is sought to ensure that the above-mentioned approaches and solutions are satisfactorily responding to the needs of the end-users and of the citizens' community at large. There is a need for an interdisciplinary approach involving contributions from technological research and socio-economic disciplines, particularly anthropology, arts, economy, law, linguistics and sociology.

Scope:

The proposed research should focus on the development of innovative solutions and technologies for urban security and resilience that, at the same time, intend to reduce the fear of crime and enhance the perception of security of the inhabitants of large urban environments.

Specific attention should be paid to technologically enhanced platforms that allow citizens both to share information and experiences in real-time streaming and to receive alerts and messages from security command and control centres.

The proposed action should take into account sustainable and low impact solutions and, possibly, rely on already set standards and tools. Modularity and security by design should also be in the backbone.

The proposed research should take into consideration past and on-going EU research in this field. The testing and validation of the results from the proposed research should be carried out in several European cities.

The Commission considers that projects requesting a contribution from the EU of between €2m and

€5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The output of this research should provide concrete suggestions for policy making to address security challenges in large urban environments.

The research results are also expected to contribute to increase the perception of security of citizens by empowering them, fostering their sense of belonging to a greater community and facilitating their engagement to improve the security conditions of smart cities.

Moreover, the research would provide new market opportunities, especially for SMEs and entrepreneurs, to develop and produce innovative technologies for urban security.

Finally, the consideration for a possible wider integration of new and existing digital technologies into sustainable and innovative security solutions is strongly welcome.

Form of funding:
Collaborative Project 100% (Capability project)

Specific call year:
This topic is part of the call for 2014.

10. Urban security topic 2: Urban soft targets protection

Specific challenge:

'Urban soft targets' can be identified as urban areas into which large numbers of citizens are freely admitted, or routinely reside or gather. Among others, these include parks and markets, shopping malls, train and bus stations, hotels and tourist resorts, cultural, historical, religious and educational centres and banks.

In ever growing urban environments, urban soft targets are exposed to increasing security threats, including cyber-attacks.

Nevertheless, in consideration of the very nature of urban soft targets, the security measures adopted to reduce their vulnerability to security threats are usually required to be softer than the ones adopted, for instance, in the context of urban critical infrastructure protection.

Scope:

The proposed research shall:

•Focus on existing tools, procedures and approaches, including smart technological devices, in order to determine best practices in urban soft targets protection.

•Develop innovative technological solutions and strategies to support cities in reducing the vulnerability of urban soft targets.

•Design and carry out large scale demonstrations of novel solutions in the field of urban soft targets protection.

The proposed actions should take into consideration past and existing researches, implemented within or outside the EU, and pay due consideration to the possible ethical issues related to this topic.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The outcome of the proposed research is expected to provide direct support to urban security policy makers and practitioners to effectively ensure urban soft target protection.

Moreover, through the expected development of innovative and smart technological solutions, the proposed research should contribute to increase the competitiveness and visibility of European security technologies and industry at a global scale.

SMEs as providers of security services and products should be in the corner stone of innovative solutions and, consequently, directly benefit from the outcome of the proposed research.

Form of funding:
Collaborative Project 100% funding (Integration Project)

Specific call year:
This topic is part of the call for 2015

11. Urban security topic 3: Countering the terrorist use of an explosive threat

Specific challenge:

Extensive research has been undertaken in recent years to enhance support to those involved in detecting and countering explosive threats. This research aims to develop methods/technologies that can be applied to each stage of a terrorist plot, including: intelligence techniques to spot those preparing for an attack; the inhibition of well-known precursors; detecting specific chemicals, and/or bomb factories and/or the Improvised Explosive Device (IED) in transit; neutralizing the IED and undertaking forensic and evidential work.

But up to now, no comprehensive research was undertaken to assess the effectiveness, the efficiency and the cost of all the developed methods/techniques. The main focus of the proposals should be to address this issue.

Scope:

Proposals should address the full time line of a terrorist explosive plot. At each period of the time line, the project should assess the effectiveness of the supporting method/technology used to counter the threat at that period using credible scenarios based on real cases, including the evaluating the most effective integration and association of existing technologies along the timeline.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The research should help those involved in counter-terrorist activities (e.g. Law Enforcement Agencies, bomb disposal units, Security & Intelligence Agencies, and Government Laboratories) to make proper choices in the application of new tools and techniques,) to make proper choices taking into account the specificities of their countries with regards to this particular threat.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2014

Ethical/Societal Dimension

12. Ethical/Societal Dimension Topic 1: Factors affecting (in-) security - Phase 1 Demo Project

Specific challenge:

Security has been defined as a subjective phenomenon that changes within society. Information on people's understanding of security issues (e. g. crime, terrorism, natural or man-made disasters), their perception of security as well as the relevant facts about the risks and dangers they face, and perceive may vary according to the level of assessment, be it public or personal (individual). Furthermore, people's feelings of insecurity and their perception of the importance of security can be different in diverse demographic groups. Persons who are amongst best protected and most secure in the society are likely to have expectations of security much higher than poorer, less protected persons.

Scope:

The action should be based on real life examples and address factors affecting public and personal assessment of (in-) security. Furthermore, taking into account past and on-going EU research, this action should aim at collecting analysing studies and data demonstrating this division. Tools necessary to reduce public and personal perception of insecurity should be examined. Proposers are also encouraged to focus on different demographic groups in order to verify how aspects such as: gender, age, income, occupation, education or kind of a lifestyle, affects the feeling of (in-) security. Furthermore, the anthropological dimension should also be considered.

Expected impact:

Better understanding of factors defining public and personal assessment of (in)security. The action should also lead at explaining how demographic background influence the feeling of (in)security. Both outcomes should help improve the strategic security planning.

The project should aim at identifying research priorities for a major real-life phase 2 project (2016).

Form of funding:
Coordination and Support Actions 100% funding

Specific call year:
This topic is part of the call for 2014.

13. Ethical/Societal Dimension Topic 2: Enhancing cooperation between law enforcement agencies and citizens - Community policing

Specific challenge:

Community policing is a value system followed by a police department, in which the primary organizational goal is working cooperatively with individual citizens, groups of citizens, and both public and private organizations in order to identify and resolve issues which potentially affect the liveability (quality of life) of specific neighbourhoods, areas, or the city as a whole. Police departments which are 'community-based' acknowledge the fact that the police cannot effectively work alone and must partner with others who share a mutual responsibility for resolving problems. Community policing aims at stressing prevention, early identification, timely intervention, as well as better crime reporting, identification of risks, unreported and undiscovered crime. Individual police inspectors are encouraged to spend considerable time and effort in developing and maintaining personal relationships with citizens and different community organizations.

Scope:

Research in this area should focus on indicating best practices for co-operation between police and citizens (communities at different level). Moreover, the proposed actions, taking into account past and on-going EU research, are expected to analyse "community policing" as an opportunity to use a community to observe their environment identify risk and exchange information.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The output of this research topic should help determine effective and efficient tools, procedures and approaches to strengthen community policing principles. This concept based on collaboration and coordinated activities should be analysed as a system aimed at facilitating information sharing and trust building. Proposers are encouraged to focus on trainings, awareness raising and information sharing activities both, for police and citizens involved. One of the most relevant impacts of the proposed research should be developing a technology (e.g. application of smart phones) which will facilitate, strengthen and accelerate the communication between two groups by making it possible for community representatives to identify the risk and immediately report it to the police forces.

Form of funding:
Collaborative Project 100% (Capability Project)

Specific call year:
This topic is part of the call for 2014.

14. Ethical/Societal Dimension Topic 3: The role of new social media networks in national security

Specific challenge:

The internet has become a central part of modem life. Omnipresent social media, especially media sharing platforms, chat sites, web forums, blogs radically change the way current societies operate. That is why these instruments attract more and more often attention from national security planners.

Scope:

This topic shall look at the role and purpose of social media and the relationship between the new social networks and national security. Research may focus on analysing the following issues:

- To what extent are social media likely to influence national security planning?
- Shall the adoption of social media across the national security community be treated as a threat or a tool for national security purposes?
- Shall the potential of social networking tools be explored by national security agencies for example in order to predict future trends or identify possible threats?

Special attention should be given to ethical and privacy aspects.

Expected impact:

Stakeholders should get a better understanding of the impact of social media for national security purposes. Proposers are encouraged to assess the positive and negative aspects, challenges and opportunities of engaging social media as well as how these tools could be used by national security planners.

Form of funding:

Coordination and Support Action 100% funding

Specific call year:

This topic is part of the call for 2015.

15. Ethical/Societal Dimension Topic 4 - Understanding the underlying social, psychological and economic aspects of the genesis, methods and motivation of organized crime (including cyber related offenses)

Specific challenge:

There is a need for a deeper understanding of processes that lead to organised crime and terrorist networks. This needs to be examined from a social science, psychological and economic perspective

Scope:

Research should investigate the role of social, psychological and economic factors in progression of individuals who had unremarkable and ordinary lives into organised crime and terrorist networks.

This research may, for instance, examine the role of friendships, kinships, milieus and peer groups of (social) networks and social media. It may also examine the characteristics of individuals that leave them susceptible to these influences and/or social conditions conducive to organised crime. The analysis may also take into account state of the art of theory and research on inclusion and social cohesion and apply economic measures (like e.g. Gini index) but also more qualitative social indicators (e.g. political participation, discrimination on the basis of race, age, class and gender). Research should also look into communication processes within and between networks as well as into processes that lead to terrorist cells.

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

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Research should lead to:

- Insights into the origins and development of organised crime and terrorist networks;
- Insights into the process underpinning the progression of individuals from non-violence into violence;
- Enhanced ability to identify individuals at risk of joining or forming organised crime

and terrorist networks;

- Enhanced ability to identify organised crime and terrorist networks in an early stage;
- Enhanced ability to prevent the emergence of organised crime and terrorist networks, and respond to the threat of existing organisations;
- Insights into ways to improve social cohesion.

Form of funding:

Collaborative Project 100% funding (Capability Project)

Specific call year:

This topic is part of the call for 2015

CONDITIONS FOR THIS CALL

Publication date: 25 March 2014 [TBC – the dates for the 2015 call are not yet clear]
Deadline: 28 August 2014 at 17:00 hours Central European Time [TBC – the dates for the 2015 call are not yet clear]

Indicative budget: [Budgetary indications are not yet possible, due to the lack of agreement in the trilogues on the overall budget of Challenge 7]

Option 1: Indicative budget : EUR XXX million from the *[Insert year e.g. 2014 or 2015, in some cases both years could be mentioned]* budget

	2014 EUR million	*2015* *EUR million*	
Topics: 5, 7, 8, 9, 11, 12	TBC	-------------------	*All single stage*
Topics: 1, 2, 3, 4, 6, 10, 14, 15	-------------------	TBC	*All single stage*

Eligibility conditions:

The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Topics 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.
Topic 8	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.
	This topic is limited to public end-users, additionally proposals should contain at least 10 public authorities from 10 different Member States.

Evaluation criteria:

The standard evaluation criteria apply. Please read carefully the provisions [*Link to the annex on standard evaluation criteria*] under Annex X before the preparation of your application.

Evaluation procedure: [*Link to the annex on standard evaluation procedure*]

- Proposal page limits and layout: 120 pages [TBC]
- Indicative timetable for evaluation and grant agreement[4]: *[as appropriate]*

[4] Should the call publication postponed, the dates in this table should be adjusted accordingly.

- specify planned date to inform applicants of outcome of evaluation, and.
- indicative date of signature of grant agreements or notification of grant decision

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements
Topics: 5, 7, 8, 9, 11, 12	15/12/2014	15/03/2015
Topics: 1, 2, 3, 4, 6, 10, 14, 15	TBC	TBC

Consortia agreements: *[as appropriate]*

[Standard sentence on climate change and/or sustainable development *[to be added as necessary]*

Disaster resilient societies

Contents

The European Union regularly suffers from natural and man-made crises and disasters, the social and economic consequences of which may adversely affect its growth and competitiveness. The growing vulnerability to crises and disasters due to likely worsening conditions of climate change, the increased probability of CBRNE accidents, pandemic or similar wide impact health threats, will have a large impact on human life, ecosystems, political and social stability, the economy and infrastructure. This leads to an increased need to improve the effectiveness of existing prevention, preparedness, mitigation and response capabilities, including in the area of critical infrastructure protection.

The objective is to reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including from extreme weather and geological events, crime and terrorism threats.

This call is divided in five parts:

1. Crisis Management and Civil protection
2. Disaster Resilience and Climate Change
3. Critical Infrastructure Protection
4. Communication Interoperability
5. Ethical/Societal Dimension

Crisis management

1. Crisis management topic 1: potential of current measures and technologies to respond to extreme weather and climate events

Specific challenge:

Extreme weather and climate events, interacting with exposed and vulnerable human and natural systems, can lead to disasters. According to the Intergovernmental Panel on Climate Change (IPCC), some types of extreme events (e.g. flash floods, storm surges, heatwaves, fires) have increased in frequency or magnitude, and in the meantime populations and assets at risk have also increased, leading to enhanced disaster risks. Besides the need for better forecasting, prevention and preparedness, improved measures and technologies are needed to better manage the immediate consequences of weather- and climate-related disasters, in particular regarding emergency responses

Scope:

Research and demonstration should focus on the potential of current measures and technologies to enhance the response capacity to extreme weather and climate events (including local measures) affecting the security of people and assets. Research should focus on emergency management operations and cover the whole crisis management, linking early warning to effective responses and coordination with first responders, including the use of adapted cyber technologies to gain time and improve coordination in emergency situations. It should also explore the links and eventual adjustments of the warning and response systems facing the observed or anticipated changes in frequency and intensity of extreme climate events, as a result of enhanced prevention and preparedness systems.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

The demo should help improving the capacity to provide adequate emergency responses to extreme weather and climate events, in particular gaining time and efficiency regarding coordination of emergency reactions in the field..

Form of funding:

Collaborative Project 70% funding (Integration Project)

Specific call year:

This topic is part of the call for 2015.

2 Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRNE contamination with dual-use applications

Specific challenge:

A fast detection of CBRNE substances using traceable tools is essential to gain time in the triage of victims in case of accidents or terrorist attack. Research on traceability and monitoring of a large number of people in case of a massive CBRNE contamination is therefore needed in order to differentiate between contaminated or not contaminated persons on-site or in hospital zones.

Scope:

The objective of this topic is to integrate existing tools and procedures along with the development of novel solutions in order to rapidly determine, in case of accidents or terrorist attack, if victims are contaminated or not (by a CBRNE contaminant) as well as the level of contamination / exposure (including making use of point of care diagnostic tests), establish a decontamination / treatment / medical follow up based on the level of contamination / exposure, ensure the tools and procedures fit in overarching search & rescue systems, establish guidelines for hospitalisation and admission to intensive care units (or other specific units) based on the contamination evaluation. The Ethical implications and social acceptance of the proposed solution needs to be studied.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Breakthrough on detection and monitoring capabilities to the benefit of first responders, civil protection and public health services. In addition, a new integrated, interoperable and centralised system approach involving all stakeholders in case of a mass contamination. Dual-use applications will be considered with possible synergies being established with the European Defence Agency.

Form of funding:

Collaborative Project 70% funding (Integration Project)

Specific call year:

This topic is part of the call for 2014.

3 Crisis management topic 3: Demonstration activity on large scale disasters' governance and resilience of EU external assets against major identified threats or causes of crisis[5]

Specific Challenge:

Governance regimes tend to lack integration when facing large-scale disaster events. State-civil society relationships, economic organization, and societal transitions have implications for disaster governance. Various measures can be employed to assess governance and resilience of major natural and man-made disasters against identified threats or causes of crisis. However, more research is needed in this nascent field of study on factors that contribute to effective governance of major crisis, including risk analysis and cost modelling. In particular, demonstration is needed to develop the concept of on-field management of international and humanitarian crises operations, including civil protection assistances, deployment (before and after a crisis) of EU teams, materials and services, possibly repatriation of EU citizens, as well as their protection and the protection of EU assets.

Scope:

The demo should demonstrate how prevention and preparedness improve the governance of disaster risk management (identifying risk areas and vulnerable groups, assigning resources to more vulnerable sites, evaluating costs of different responses, etc.). The demo would aim at demonstrating the EU capability to develop, test and validate crisis management systems which could be applied in real situations outside the EU. The research should take into account the consequences of poor and/or late situational awareness reducing the ability to comprehend the scale of a crisis and explore the advantages, saving costs and assets, of comprehensive risk prevention systems versus the forer approach; it should also consider the whole management chain from the detection of a crisis event to the delivery of information to the remote centre from here to the responders on site, moving through the mobilization of responders and support of field users, the planning of actions and the prioritization of efforts within emergency scenarios, combining dynamic data (from sensors, aerial networks etc.) with static information (maps, infrastructure, assessment templates) enabling a better risk assessment and improved decision-making. Interoperability and dual-use applications should be considered as well as health, environmental, climatic, legal and ethical aspects.

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

[5] For further information please consult the Security Research and Industry reference document available at http://ec.europa.eu/enterprise/polilcies/security /document/index_en.html

logistics. It should also increase our capacity to respond to disasters potentially affecting EU external assets.

Sound governance and a good knowledge of resilience factors are crucial during large scale disasters due to the involvement of a large number of actors and the uncertainty and lack of information that characterises major identified threats or causes of crisis. This is even more acute for situations outside the EU. In order to prepare solutions for an improved coordination, the demo should identify and take into account comprehensive and representative scenarios that will trigger as many aspects of the different crisis situations as possible, involving the tactical, operational and strategic level.

The population is always a key actor in crises and disasters, both as the affected and as the very first source of response. Enhancing the disaster resilience of societies in relation to EU external assets means first and foremost preparing the population, thus a strong citizen focus should be an important driver of the demo. In this sense, social networks and their particularities in terms of communications could be taken into account, in particular in the way they can be used for improving large scale disaster's governance.

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

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

A large set of FP7 projects related to crisis and disaster management have been completed or launched in recent years within the EU. In addition to this, national experiences have also been built and evaluated in this field, providing a wide range of findings which should be taken into account in the demonstration. The demo should therefore build on existing tools and results of completed and ongoing projects, and combining them with legacy systems and tools. Knowledge and experiences from other fields such as health, environment, climate change, transport etc. could be useful and could be brought into the demo if relevant. Finally, lessons learnt from past incidents, preparedness activities and simulations should also pave the way for future actions since lessons learnt are key in improving the system.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

The demo would aim at demonstrating the EU capability to develop, test and validate crisis systems which could be applied in real situations outside the EU, following the EU approach to resilience (i.e. involving prevention, preparedness, response), also in line with the EU and the UN approach to Disaster Risk Reduction, which also gives greater importance to integrating adaptation to climate change and disaster risk management.

This should impact on the rapidity of assessment and feedback of data to coordination centres, effective communication and coordination of response actions and sharing information with the public. This would certainly contribute to boost the competitiveness and visibility of EU crisis services and product suppliers.

The demo should correspond to EU policy priorities in the area of disaster's governance and resilience, where serious major identified threats or causes of crisis require immediate action; situations that may affect the lives, infrastructures, the environment or the basis values of EU external assets.

The demo should in particular contribute to the general orientations of the post-2015 framework for disaster risk reduction (HFA2) coordinated by the United Nations International Strategy for Risk Reduction in which the EU is a working party. It will also support the EU Civil Protection policy orientations set in the Commission 2010 Communication *'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance'.*

Form of funding:
Collaborative Project 70% funding (Demonstration Project)

Specific call year:
This topic is part of the call for 2015

4 Crisis management topic 4: Feasibility study for strengthening capacity-building for health and security protection in case of large-scale pandemics – Phase I Demo

Specific Challenge:

Emerging diseases and their pandemic potential pose a great security threat at national and EU level, particularly in the era of globalization when disease can spread more rapidly than in previous eras. Thirty four percent of all deaths worldwide are now attributable to infectious disease, while war only accounts for 0.64 percent of those deaths. Improving capacity-building is key to fight epidemics and the European Union must increase its efforts to improve domestic and global risk assessment, surveillance, communication capability and governance. Additionally, reducing disease transmission through public education and related measures is also crucial to minimizing pandemic impacts, i.e. for health security and protection in case of large-scale pandemics, further capacity-building is essential.

Scope:

Based on the consolidation and exploitation of results, tools and systems from previous R&D efforts and building on existing projects, the overall aim is to develop innovative concepts. Approaches should integrate relevant research as well as aspects related to risk assessment, communication and governance. Concepts should be developed with a view to cross-border approaches. The project should aim at identifying gaps and research and priorities to be addressed in a second phase focusing on demonstration.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Identification of research gaps and priorities for improving capacity-building at transnational level with a view to prepare for a demonstration project including all relevant actors, including SMEs.

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014

5 Crisis management topic 5: Situation awareness of Civil Protection decision-making solutions – preparing the ground for a PCP

Specific challenge:
The Lisbon Treaty contains specific and important changes regarding Civil Protection that provide competence to the EU to: a) carry out actions to support, coordinate or supplement the actions of Member States at national, regional and local level in risk prevention and preparation; b) promote swift effective cooperative action within the EU between national civil protection services; c) promote consistency in international activities, including transnational crisis management. A comprehensive European approach on security issues based on the capitalization of knowledge existing at EU and national will considerably help the development and implementation of harmonized Civil Protection decision-making solutions.

Scope:
The study should carry out a survey leading to a mapping of new and promising civil protection decision-making solutions developed in the 7th Framework and national programmes in transnational crisis and disaster management situations, including in fast developing and changing crisis situations.

This should prepare the ground for a future PCP for civil protection solutions, including public-private cooperation at local, national and EU level, with a view to test technological solutions and protection, deployment and intervention equipments (e.g. tents, relief equipments, basis needs supply, Remotely Piloted Air System (RPAS)) and tools (e.g. situation awareness) in order to make them more cost effective and interoperable.

This coordination action should thus:

- exchange experiences between (public) stakeholders on civil protection and create a network of potential procurers;
- initiate a concrete debate on the mid-to-long term public needs that would require the development of new civil protection technology solutions with a potential role for pre-commercial procurement strategies; and
- create a roadmap for a future PCP topic to be included for an upcoming Horizon 2020 secure societies research call.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Preparing the ground for a PCP, improvement of emergency responses with better knowledge of existing technological solutions, perspectives for large testing of civil protection solution with the view to improve decision-making solutions at national and European levels.

Proposed instrument:

Coordination and Support Action 100% funding

Specific call year:

This topic is part of the call for 2014

Additional condition:

At least 3 Member States relevant public authorities

6 Crisis management topic 6: Addressing standardisation opportunities in support of increasing disaster resilience in Europe

Specific challenge:

Increasing Europe’s resilience to crises and disasters requires an orchestrated set of actions across the value chain, including standardisation. While dedicated research projects and new topics look into different aspects of resilience to be investigated and further developed, at the same time related opportunities and needs for European standardisation to support disaster resilience have to be addressed. Such standardisation activities could e.g. significantly improve the technical, operational and semantic interoperability of command, control and communication systems for crisis and disaster management, or the interoperability of detection equipment and tools in the areas of CBRNE. Research should support the identification and further elaboration of potential standardisation opportunities and needs in those technological areas where a significant contribution to improve the disaster resilience in Europe through standardisation can be expected.

Scope:

Proposals could address the areas of crisis management / civil protection and/or CBRNE, including sub-sets of both areas. Proposals need to assess the feasibility and the expected impact of the proposed standardisation activity, the appropriate standardisation deliverable(s) and the expected time frame to finish the proposed activity. Relevant legislation on EU and Member State level need to be taken into account appropriately, including potential ethical, societal and privacy issues of the proposed activities. Proposals need to show how duplication of efforts with relevant past or on-going EU research projects, and standardisation activities on European (e.g. CEN/TC 391) and international level (e.g. ISO/TC 223) will be avoided: how proposed activities will be coordinated with other, relevant activities like e.g. the EU action on enhancing the resilience of infrastructures[6], how a cross-fertilisation of work between the proposal and these relevant activities will be achieved and how the proposal consortium intends to involve itself in relevant CEN and/or ISO TC's.

Expected impact:

Improved disaster resilience of EU population, crisis management / civil protection and/or CBRNE systems, tools and services, and reduced fragmentation of the respective EU market(s).

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Proposed instrument:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2015

7 Crisis management topic 7: Accelerated Open topic for Small and Medium Enterprises: "Combating biological threats"

Specific challenge:

The accidental or intentional release of pathogenic viruses or bacteria in densely populated areas could have catastrophic consequences. Biothreat agents can be dispersed in air, water or food and are extremely difficult to detect, identify and remove. In the event of a biological attack of other contamination incident, fast and reliable detection and decontamination tools have to be made available to laboratory technicians, including the collection of samples in the field and delivery to the laboratory. SMEs are at the front edge of the development of detection devices for dangerous pathogens and of decontamination tools for personnel and/or facilities in the event of accidents or terrorist attacks threatening security. Proof of concept of existing prototypes developed by SMEs is needed to demonstrate their applicability with a view to boost their near-term commercial impacts.

Scope:

The objective is to carry out small-scale demonstration of detection and decontamination tools for dangerous pathogens with a focus on prototypes developed by SMEs.

[6] COM(2013) 216 final, An EU Strategy on adaptation to climate change, Action 7: Ensuring more resilient infrastructure

For each project/consortium, the following recommendations apply:

- at least 70% of the EU funding should go to eligible SMEs;

- small-sized projects are encouraged (up to € 1.5 million EC Funding);

- the project duration should be between one and two years;

- small consortia (3-7 partners) are encouraged;

- SME coordinators are encouraged but they are by no means mandatory – lack of prior FP7 experience should not be seen as a handicap for an SME coordinator; and

- at least one end-user should be included in the consortium.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Projects should enable to accelerate innovation and reduce time to market. It is expected that solutions with potential for significant near-term commercial impact will be developed. Potentials for spin-off applications in non-security sectors will be considered as positive.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

It is also expected that through this topic SMEs will play a more active role in the development of new innovative technologies and solutions.

Form of funding:
Collaborative Project 70% funding (Capability Project)

Specific call year:
This topic is part of the call for 2014

8 Crisis management topic 8: Crises and disaster resilience – operationalizing resilience concepts

Specific challenge:

To increase Europe's resilience to crises and disasters is a topic of highest political concern in the EU and its Member States. While the term 'resilience' can be described as "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." (UNISDR, 2009), it is necessary to break down and practically apply this definition to the different security sectors. Resilience concepts namely need to be developed for critical infrastructures (supply of basic services like water, food, energy, transport, housing/ shelter, communications, finance, health), but also for the wider public to integrate and address human and social dynamics in crises and disaster situations, including the role of the media. Resilience concepts need also to take into account the necessity to anticipate, to plan and to implement in the crises time a substitution process aiming to deal with a lack of material, technical or human resources or capacities necessary to assume the continuity of basic functions and services until recovery from negative effects and until return to the nominal position.

Resilience concepts need also to take into account the necessity to anticipate, to plan and to implement a substitution process in a crisis or disaster, aiming to deal with a lack of material, technical or human resources or capacities necessary to assume the continuity of basic functions and services until recovery from negative effects and return to the normal situation. Moreover, as resilience management and vulnerability reduction are closely related, it is necessary to link the on-going efforts to harmonise and share EU-wide risk assessment and mapping approaches[7] with relevant resilience management approaches, to ensure that risk assessment is followed by the development of resilience concepts in the various security sectors, based on the results of the risk assessments.

Scope:

Research should first survey worldwide approaches how to define, develop, implement and evaluate resilience concepts, including relevant EU sectoral approaches. In a second step, promising implementation approaches and elements should be identified which can be adapted to one or more of the above mentioned critical infrastructures, and/or the public, and assessed regarding their potential to serve as a basis for a general guideline on resilience assessment and implementation. In a third step, such a general resilience management guideline should be developed, linked with the EU Risk Assessment Guidelines, and operationalized in one or more of the security sectors, and/or the public. The successful pilot implementation of the developed guideline need to be demonstrated and tested in an operational environment, e.g. Air Traffic Management, electricity grids, gas transmission networks or space infrastructures. This pilot implementation should include a dedicated risk assessment and risk management approach, addressing e.g. the issue of cascading effects. Proposals need to show that the proposed research does not overlap with activities proposed under the current *"Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"* (CIPS) [8] programme and its successor in the Internal Security Fund, and that it is linked to the *"European Programme for Critical Infrastructure Protection"* (EPCIP) programme[9] and its new revised approach. Findings from relevant FP7 projects need to be taken into account, and integrated into the research where possible. Furthermore, a close collaboration with the major EU demonstration

[7] SEC(2010) 1626 final, Risk Assessment and Mapping Guidelines for Disaster Management

[8] Decision 2007/124/EC, Euratom, OJ L58 of 24.2.2007, establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks' (CIPS)

[9] COM(2006) 786 final, On a European Programme for Critical Infrastructure Protection

project on aftermath crisis management (SEC-2013.4.1-1, expected to start in 2014) should be sought, in order to avoid duplication of efforts and to facilitate cross-project contributions.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

The proposed research should for the first time develop a European Resilience Management Guideline, which through its pilot implementation should facilitate the uptake of risk assessments through Member States and Critical Infrastructure Providers to increase their crises and disaster resilience, in a more coherent way.

Form of funding:

Collaborative project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2014

9 Crisis management topic 9: Trans-national co-operation among National Contact Points (NCPs) for Security

Specific challenge:

As a complement to the cross-cutting NCP networks focussing on quality standards, benchmarking and legal/financial training, the Security NCP network should focus on sharing good practices related to security specific issues, and in particular in the area of crisis management.

It could also facilitate contacts with Third Countries contact points.

Scope:

The action will focus on identifying and sharing good practices. It may entail joint workshops, technical training on security specific issues, such as crisis management. The Security NCP network should also organise trans-national brokerage events on a regular basis and on the demand of the Commission. The proposal should include an in-depth mapping of security research national systems for crisis management. It should facilitate partner search, also via its Third Countries contact points.

Expected impact:

The establishment of the NCP network should lead to an improved NCP service across Eu-rope and provide security specific information to the security research community. This means that the outcome of the NCP project should be available to all NCPs independent of whether or not they are beneficiaries in this project. The service shall also support the net-working between the research community and end users in the specific domain of security.

Form of funding:

Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014

10 Crisis management topic 10: Intervention forces tracking

Specific challenge:

Intervention forces in humanitarian mission are quite often at risk due to the instability of the countries of deployment and possibly due to the action of adversary forces still trying to gain the control of the country, the population and offered support. Security of these intervention forces is of a paramount importance.

Scope:

Proposals should address the problem of tracking the assets and the staff of the deployed mission in third countries in CSDP context. Real-time tracking may help to reduce the exposure to security risks of these missions. The solution proposed should integrate and/or complement seamlessly the used communication system (either standard or specific) and, if any, the Control and Command system in place (even if abroad).

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Increase the security level of civilian CSDP missions.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

Disaster Resilience & Climate Change

11. Disaster Resilience & Climate Change topic 1: Co-ordinating research and innovation activities on climate change adaptation and disaster risk management in Europe

Specific challenge:

Climate change adaptation and the management of risks from extreme events are emerging as key research priorities both at EU level and internationally. A wealth of knowledge already exists regarding the assessment of climate-related vulnerabilities and risks at different geo-climatic and socio-economic contexts, supporting cost-effective adaptation and long-term risk reduction. In the light of new achievements and information on climate-related impacts and adaptation requirements, there is an emerging need for the coordination of research activities, and the development of communication mechanisms among the scientific community, practitioners and decision- and policy-makers at different scales.

Scope:

Develop a platform to organise consultations and facilitate dialogue among different stakeholder groups at the EU level and at different geographical scales, throughout the duration of Horizon 2020, paying due attention to international developments in the field. With the aim of better coordinating research, emphasis will be placed on supporting clustering and close cooperation among international, EU and nationally funded initiatives in the field of climate change adaptation, bringing together scientific, technical and socio-economic information. Foresight activities to identify key knowledge gaps, also considering the requirements of the recently adopted EU Climate Change Adaptation Strategy and national risk assessments, must be employed as means to prioritise and mainstream research to address decision-making challenges. A proper planning of dissemination activities, encompassing large-scale events to foster the science-policy interface across the EU should be envisaged.

Expected impact:

Better coordination of research and innovation activities on climate change adaptation and long-term reduction of vulnerability to extreme weather events in Europe, in cooperation with the Climate JPI and the EIT. Synergies among international programmes (e.g. UNEP/PROVIA), EU-funded and Member State-funded research. Better dissemination and communication of key research findings to fill knowledge gaps. Support to implementation of the EU Adaptation Strategy and relevant national efforts.

Proposed Instrument:

Coordination Action 100% funding

Specific call year:

This topic is part of the call for 2014

12 Disaster Resilience & Climate Change topic 2: Towards large-scale deployment of technological and non-technological adaptation options and practices for key European systems and economic sectors

Specific challenge:

As the EU and Member States progress towards the development of appropriate responses for adapting to climate change, there is a pressing need to provide the appropriate evidence base to support the replication of successful adaptation and long term risk reduction options. New or adapted solutions, fine-tuned to specific natural and socio-economic conditions, are needed in order to protect and reduce the vulnerability of sensitive resources, economic sectors, infrastructure and society fromclimate-change related threats (long term changes and extreme weather events of increasing frequency/severity).

Scope:

Innovative, cost-effective solutions will be developed to contribute towards climate change adaptation by enhancing the resilience of key economic sectors to the impacts of climate change including climate-proofing critical infrastructure assets and systems. Demonstration projects should aim to develop, test and disseminate technological and non-technological options, including eco-system based approaches, to address climate-related risks in different geo-climatic and socio-economic contexts. They should build on the coherent assessment of vulnerabilities and future climate change impacts considering uncertainties, monitoring of performance and effectiveness, post evaluation requirements as well as operational and organisational/governance requirements. Proposals should demonstrate synergies with major implementation projects at local, regional or national levels and strengthen complementarity with other EU funding mechanisms, particularly with the EU Structural Funds.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Market uptake of technological and non-technological climate change adaptation solutions with high replicability. Rapid large-scale deployment of innovative options for adapting to climate change. Enhanced resilience of key European economic sectors and services to natural disasters and extreme events.

Proposed Instrument:

Collaborative Project 70% funding (Capability project)

Specific call year:

This topic is part of the call for 2014

13 Disaster Resilience & Climate Change topic 3: Natural Hazards: Towards risk reduction plans at national and European level

Specific challenge:

Research on natural hazards in the last 10 years has covered several fields related to concepts, methods and tools for hazard and risk assessment. Policy development has now stimulated more prevention, preparedness and sustainable management. Recent catastrophic events have also demonstrated that society has become more vulnerable and exposed to risk. A more coherent approach to threat and related risk management including multi-risks and possible cascading effects now need to be better taken into consideration. There is therefore a strong need to organise and structure, with all the relevant actors, a new strategy for future research activities in natural hazards focusing in particular on methods, procedures and content for a better risk reduction strategy at more adequate spatial and temporal scales. It will be necessary to go beyond the traditional risk concepts and also include resilience and systemic and time-dependant vulnerability.

Scope:

The overall idea is to develop a new strategic vision on natural hazards risk reduction building on new concepts and using effective mechanisms and interactions with the key players (e.g. scientists, authorities, users, civil protection, UNISDR platforms...) for identifying the necessary key actions to be promoted (short to long term perspective) in order to improve scientific knowledge and apply or adapt current tools and methods to a new and effective risk reduction strategy at national/European level. This would take into account the EU and national adaptation strategies as well as the developing disaster risk management planning done at national or appropriate sub-national level.

Work will therefore gain from capitalising on previous actions at EU and national levels and must lead to a reduction in the uncertainties which currently characterize natural hazard models, include cascading effects and multi-risk concepts able to translate risk analysis into loss (consequence) analysis and resilience indicators, and use risk assessment models able to operate at different scales. Natural hazard events triggering other natural hazards or technological disasters should be part of the overall conceptual approach. New development needs on vulnerabilities, risks, prevention, mitigation, adaptation and sustainable risk management need to be taken on board in this approach.

Expected impact:

Consolidation of and enhanced synergies between European and Member State funded research and innovation activities in natural hazards/disasters risk reduction. Contribution to the development of a strategic science agenda in this field.

Proposed instruments:

Coordination Action 100% funding

Specific call year:

This topic is part of the call for 2014

14 Disaster Resilience & Climate Change topic 4: Opportunities, costs, impacts and risks of adaptation measures and policies in key economic sectors and services in Europe

Specific challenge:

In order to further support adaptation to climate change in different contexts and scales (from local to regional, national and EU), there is a need for a more standardised basis (including transferable, widely applicable tools and methods) for assessing potential climate change impacts, vulnerabilities, risks and opportunities, and providing information relevant to different target groups and stakeholders. Furthermore, the knowledge base needs to be strengthened through a more coherent approach to the identification and assessment of the performance and impacts of different adaptation measures, considering uncertainties, costs and benefits in order to better inform decision and policy-making. Cascade impacts and the indirect cross-sectoral effects of adaptation responses are also of particular importance, with a view to providing a more holistic approach to and understanding of climate change adaptation requirements and implications across the European economy.

Scope:

The aim is to develop standardised methods for assessing adaptation measures (technological and non-technological options) to address vulnerabilities and risks related to long-term climate change and extreme events for European sectors of particular socio-economic and environmental significance. Methods should be integrated into state-of-the-art decision support tools and tailored to facilitate decision-making by different end-users (e.g. individuals, businesses, local authorities and planners, governments). They should facilitate a coherent approach to the assessment of adaptation options, their implementation timeframe, their direct and indirect benefits and costs, also considering cross-sectoral and other potential spill-over impacts of their implementation. Research should advance existing efforts and exploit current knowledge and local practice on impact, vulnerability, risk and the assessment of adaptation options across different socio-economic sectors and geo-climatic contexts.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Better science-based decision making on climate change impacts, risk vulnerabilities and relevant options to address them, based on a coherent and standardised basis for decision support, tailored to the needs of different target groups. Improved quantification assessment of the opportunities, costs, risks and impacts of adaptation to climate change. Enhanced implementation of the EU Adaptation Strategy and national and local efforts towards climate-proofing.

Proposed instrument:

Demonstration Actions 100% funding (Integration project)

Specific call year:

This topic is part of the call for 2014

15 Disaster Resilience & Climate Change topic 5: Natural Hazards: towards operational forecasting and early warning capacity

Specific challenge:

In seismically vulnerable regions and cities, building codes and retrofitting actions have helped to mitigate the risks related to earthquakes. Unfortunately they are still not always implemented or are difficult to put in place for various reasons, for example in old historical centres. Other methods or tools therefore need to be developed to protect cities and citizen. Early warning and operational earthquake forecasting are both part of these potential new tools that are being developed mainly in the US and Japan and also now in Europe. However, the new goal is short-term. The 'practical' applications of short-term forecast, early warning methods, time dependent vulnerability estimates and rapid loss assessment for earthquake risk reduction are still far from being operational and need therefore strong international scientific collaboration to make substantial progress.

Scope:

Within a rational short term mitigation strategy the idea and goal is to reach an effective real time seismic risk reduction capacity. [In this context, it will be important in the field of forecasting to: decrease physical and systemic vulnerability, to provide complete (probabilistic) information useful for making operational decisions.] The approach will explore how to move from single model hazard forecasting to 'ensemble' models, further our understanding of what is happening in the preparatory phase of a large earthquake, and move from probabilistic hazard forecasting to short-term risk forecasting. For early warning, a new generation of systems need to be elaborated integrating innovative technologies or networks with social network data. Effective methods and clear structure to communicate scientific results and mitigation information to the relevant actors, authorities and public officials at the relevant steps will need to be fully integrated into the process.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

More reliable earthquake risk prediction/forecasting models. Improved short-term forecasting, real operational forecasting, and fast, reliable alerts and information. Better communication on forecast and early warning to users and the public. Tangible reduction of human and economic losses.

Proposed instruments:

Collaborative Project(s) 100% funding (Capability project)

Specific call year:

This topic is part of the call for 2015

16 Critical Infrastructure Protection topic 1: Critical Infrastructure “smart grid” protection and resilience under “smart meters” threats

Specific Challenge:

Critical Infrastructure functions are technologically and operationally interconnected, of which their exact possibilities and potential risks need to be better understood. For example: in the case of energy distribution networks, especially “smart grids”, the massive proliferation of "Smart Meters" as mandated by the Third energy Package introduces new threats.

Scope:

The objective is to analyse potential new threats generated by the massive introduction of“smart meters” on the distribution grid system and propose concrete solutions in order to mitigate the risks, improve resilient and reduce vulnerability of critical infrastructure “smart grid”, due for example to cyber-attacks, or to the locally diffused interconnectivity with renewable energy grids, and the existence of widely spread entry points that could locally influence the energy grid and its functioning.etc.

The new technologies, processes, methods and dedicated capabilities shall help protect the energy distribution grid infrastructures and shall also take into account the urban areas implications (i.e. the general public subscribing to this service). The research shall provide concrete solutions for securing public and private critical networked infrastructures and services against the above mentioned threats.

It is expected that consortia under this research topic will select the most representative sample of “smart meters” used in Europe’s smart grid as starting point of the research and analyse their potential weakness/threats.

Moreover the proposal shall study and provide solutions in order mitigate the impact of “smart meters” on the current critical infrastructure security and resilience to new threats.

It should take into consideration the work completed to date by the the Smart Grid Task Force Working Group 2, concerning the cyber security assessment framework and the related Best Available Techniques there defined.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately.

Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

It is expected that the research output will lead to a systematic approach to resilience enhancements of smart grid critical infrastructures when new components are added. Furthermore a small scale proof of concept of system should be created in order to demonstrate the “resilience” of the proposed “solutions”.

Finally the research should be carried out in the context of policy initiatives at EU level on the Smart Meters and Smart Grids, such as the 2011 CEN/CENELEC/ETSI Mandate 490 on smart grids (including the security and data privacy issues on the roll-out of smart metering systems), and the 2009 CEN/CENELEC/ETSI Mandate 441 on smart meters, as well as the guidance on software in smart meters, provided by WELMEC.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

17. Critical Infrastructure Protection topic 2: Demonstration activity on tools for adapting building and infrastructure standards and design methodologies in vulnerable locations in the case of natural catastrophes

Specific challenge:

The expected increase of frequency and severity of climate-related natural catastrophes and the current risks of disasters of geological origin pose a serious threat to buildings and physical assets located in vulnerable locations, including critical infrastructures (i.e. public buildings, such as governmental offices, transport stations, terminals and historical buildings and monuments) along their life cycle. One of the responses to be better prepared to crises related to natural hazards is to adapt building standards and infrastructure in order to limit the risks of demolition, protect critical infrastructure and save human lives in the case of a major event. Complementing current research in this area, and based on the knowledge of risks in vulnerable areas in Europe, building standards should be developed and tested, applying a number of technological means and design procedures.

A comprehensive approach should be developed that take into account the security issue from the conceptual design of any building to its operation (in the case of a critical infrastructure) or use (in the case of households). Cascade failure of interconnected infrastructure assets (installations for energy, transport, water, ICT) due to co-location or hub-functions needs to be avoided. The comparison of different solutions tested should include cost and cost/benefit analyses, and societal implications.

Scope:

The research proposal shall develop methods and tools for adapting building and infrastructure standards and design methodologies in vulnerable locations to climate-related impacts and/or other natural hazards. Furthermore the research proposal shall demonstrate its finding, taking into account the occurrence of different types of natural (climate or geological) hazards, and including comparative cost and cost/benefit analyses.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The development of building standards and design methodologies for infrastructures and households located in vulnerable areas will have a clear impact on security of citizens and assets).

The topic will complement FP7 research focusing on impacts of extreme weather on critical infrastructure.

Form of funding:

Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

18. Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator - analysis and development of methods for assessing resilience

Specific challenge:

A better understanding of critical infrastructure architecture is necessary for defining measures to achieve a better resilience against threats in an integrated manner including from natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks).
Moreover a global approach of the resilience on the critical infrastructure should be taken into account, inclusing: human factors (i.e. radicalization), security issues, geo-political issues, socio economic issues, etc. and increased vulnerability due to changing natural disasters.

Scope:

Critical Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The analysis of resilience should therefore not only focus on potential threats caused by attacks or accidents (human error or terrorist/criminal attacks), but also on the expected developments in these areas and the impacts and potential challenges of new technologies.

Therefore the effectiveness of a resilient critical infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event (be it natural, human error or terrorist/criminal attacks). The proposed research shall demonstrate that a set indicator could be applied to critical infrastructures in order to assess its level of "resilience", moreover a scale approach of "resilience" level should be proposed across critical infrastructures (power grid, water, etc.).

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Therefore the proposed research should analyze different areas of critical infrastructures (energy grid, water supply, transport, communication, etc.) and propose a comprehensive methodology that uses uniform and consistent data from known Critical Infrastructure Protection threats in an integrated manner to develop a resilience level based on summations of various "indicators" (technical and non-technical, i.e. human factors).

Furthermore the proposal research outcome should select at least two types of critical infrastructure as test case and apply the above methodology in order to demonstrate its applicability.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

19. Critical Infrastructure Protection topic 4: Protecting potentially hazardous and sensitive sites/areas considering multi-sectorial dependencies

Specific challenge:

There is a need to better understand how society as a whole might be affected by risks of accidents, natural disaster or terrorist attack on sensitive sites/areas (involving potentially hazardous substances), in order to enable effective protection measures to be developed. In this respect, the breadth of impacts from Seveso type sites/areas has to be investigated, considering multi-sectoral dependencies (notably transport, energy, communications, water). This implies developing knowledge on multiple types of sectors and socio-economic conditions around Seveso type sites/areas that might be affected by accidents, taking into account the type of sites/areas, CBRNE substances of concern, the vulnerability of various sectors and their dependencies/interactions and of the population, and scenarios mimicking different levels of severity of impacts.

Scope:

Research should include analysis of risks and strength/vulnerabilities, identification of alternatives resources and focus on the development and testing of qualitative methods that involve identifying links between sectors (multi-sectoral dependencies: systems and connection nodes definition and modeling) and evaluating how impacts from a Seveso typeaccident might affect them (cascades effects). Quantitative impact assessment tools should also be developed to evaluate socio-economic impacts of such accident. Research outputs should enable to improve or design protection measures (including people formation) for a better preparedness to Seveso type site/area related accident. Small-scale demonstration activities focusing on SMEs should be considered.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

The research and demonstration should enable to help policy-makers and other stakeholders to understand how multiple sectors, community, region or nation could be affected in total by an accident from a Seveso site/area, and what the total impact might be (material, human, economic). This can be useful to understand the potential severity of a CBRNE accident decrease the cost of this kind of crisis and develop adequate protection measures in the light of established policy goals. In addition, risk assessment studies should enable to evaluate different sectors, regions or populations compare them in terms of relative vulnerability to help set priorities that can guide the allocation of protecting measures financing appropriately.

Form of funding:

Collaborative Project 70% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

20. Critical Infrastructure Protection topic 5: Cybercrime on Industrial Control Systems protection

Specific challenge:

Industrial and Automation Control Systems (IACS) constitute the foundations of key strategic and critical sectors according to the Council Directive 2008/114/EC and the EU Internal Security Strategy, such as Energy, Oil and Gas, along with Water and Chemical. Those sectors provide a critical service to citizens and countries and the threat of sabotage through a specific and lead driven attack may represent a major drawback to an individual or to the Economy. Electricity service, for instance, is crucial because involves more than a country.

Scope:

IACS are no longer isolated siloes, they are fully integrated with corporate ICT infrastructures. Despite this strong connection between the two infrastructures, there is only little awareness regarding ICT risks that can affect IACS. An attack to ICT assets can spread to IACS jumping to SCADA and Control Centers.

In order to increase European Critical Infrastructures resiliency and availability, new approaches are needed. IACS and SCADA design does not address cyber-attacks and IT risks by conception. Their vulnerabilities are therefore easily exploitable.

To reduce such vulnerability, aside integrating defence from cyber-attacks and IT risks into IACS and SCADA design by conception, a parallel and integrated approach based on distributed and local intelligence may be adopted.

This topic aims at designing and developing approaches to SCADA and IACS security based on the synergic integration of ICT security technologies into SCADA and IACS and the development and/or exploitation of local intelligence embedded inside different kind of mechanical systems (pumps, engines, etc.). The logic controls embedded in mechanical systems may be exploited to further develop autonomic behaviours capable of overriding or differently executing orders from the IACS, so to isolate and neutralize not only hazardous accidental commands, but, as well, malicious orders actually generated by cyber-attacks.

Attention should be paid as well on how to extend existing published standards and methodologies to address the new threads for IACS modus operandi scenario.

European Critical Infrastructures, operating locally or internationally, should be the end users, especially those named European Critical Infrastructures by the Council Directive above.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

European industry will benefit from cyber security improvements due to present and future cyber-attacks protection, increasing availability and resiliency, showing a stronger state to dissuade penetration attempts.

The European Economy will avoid adverse panic situations after cyber-attacks against key economy actors

SMEs will provide specific and very focused security services such as fine tuning, security assessments, threads surveillance and many more are essential to ensure a successful and innovative solution. Liaison should be done with previous security research.

Form of funding:
Collaborative Project 100% funding (Capability project)

Specific call year:
This topic is part of the call for 2015

21. Critical Infrastructure Protection topic 6: Improving the aviation security chain

Specific challenge:

Aviation Security is governed by EU legislation and implemented at airports (checkpoint for passengers and staff, hold baggage and cargo control areas, etc.) and to relevant supply chains. The security requirement is to prevent unlawful interference with aviation security through aircraft, from which stems the requirement to prohibit dangerous items such as arms and explosives ('the prohibited items') coming on board an aircraft, be they carried on people, in their items, or concealed as air cargo or mail as well as supplies. Maintaining the integrity of security restricted areas for persons, items, consignments and supplies, from the moment they were controlled until they enter a secured aircraft is vital.

Policy is moving towards more risk-based, outcome-focused, passenger-facilitation oriented measures.

The challenge for aviation security research shall be to explore new ways and ideas that are conceptually very different to those already in development or deployed. This shall lead to designing systems and processes that are faster, more accurate and reliable, less invasive, and overall more efficient to operate than existing ones.

Examples of elements to visions for the future of aviation security are outlined in the COPRA FP7 project[10], Flightpath 2050[11] and IATA check point of the future[12].

Research under this topic needs to go beyond advising on current operations which are improved through short and medium term (below a 5-7 years' time horizon) action. It should therefore

[10] COPRA Aviation Security Research Roadmap: http://www.copra-project.eu/Results.html

[11] Flightpath 2050: Europe's vision for aviation:
http://ec.europa.eu/transport/modes/air/doc/flightpath2050.pdf

[12] IATA Checkpoint of the Future: http://www.iata.org/whatwedo/security/pages/checkpoint-future.aspx

investigate systems which will translate the mentioned objectives into operationally viable processes which have an identifiable exploitation path for operators to use. It should also explore novel opportunities for security interventions and how current processes could be re-designed to give an equivalent security outcome but better passenger experience or simplification of industry processes. It could investigate how to merge other security activities or (passenger) controls with aviation security. It may test opportunities to integrate different processes into a better overall system, including at local, national, European and global level.

Scope:

While research should deliver solutions for higher levels of security and facilitation it should be developed and tested to assess their impact and viability. Realistic estimations and cost-benefit analyses of proposed solutions, both from a governmental as well as from an industry point of view, should be included to help identify promising and reasonable approaches. The legal implications of any proposal should also be assessed, especially for health and safety, but also under data protection and non-discrimination principles.

Possible areas of research (not exclusive) could be: alternative screening processes and interventions; investigate how, where and when aviation security controls shall take place to provide the most effective and efficient results; look at the further development of processes' to maximise security outcome and minimise impact on industry and passengers; and how compliance and their effectiveness will be demonstrated. It should include system level solutions.

It could touch on technical areas such as:

integrated technologies and processes; the use of artificial intelligence; technologies and methods to screen items/people at a distance; radically new sensor technologies; networked information sharing; passenger tracking; automation; data/sensor fusion; self-verification systems for compliance monitoring; procedures should noxious gases accidently (or otherwise) be released on-board a plane; and integrated alarm resolution.

The effective implementation of any approaches should be explored through well recorded testing and trials. Trials should identify if any of the benefits are possible; if the process may introduce any vulnerabilities; and how compliance with such approaches could be assessed. Findings from relevant on-going FP7 projects should be taken into account.Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

Successful new approaches leading to a higher level of security and a reduced operational impact on passengers and industry that prove to be effective and efficient throughout their live time.

Form of funding:

Collaborative project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2014

Communication technologies and interoperability

22. Communication technologies and interoperability topic 1: Information management, systems and infrastructure for civilian CSDP missions

Specific challenge:

Considering the range of civilian CSDP missions in complex environments, the ability to efficiently manage information and resources is a key factor in all the phases of crisis management, from early warning up to "the-lessons-learned' phase, and the discontinuing process throughout. There is a need to research C2 (Command and Control) processes, information management, systems and infrastructure within the context of CSDP with a view to developing coherent and interoperable processes, tools, technologies and capabilities to improve the planning and conduct of crisis management operations.

The development of a Situational Awareness and Operation Control Platform (SAOCP) will improve cooperation among different EU actors and with Member States, with the possibility to involve also other international organisations, and in particular EU partners in crisis management, notably UN, NGOs, etc.. The needs of end-users will be a focal point of the proposed coordination action.

Scope:

Proposals should address the development of a specific and dedicated research agenda, including the technical specifications which will serve as basis for the future development of a Situational Awareness and Operation Control Platform (SAOCP). This platform should allow end-users to enhance their common understanding of crisis management in EU civil CSDP missions. It should also improve the management of the EU resources' allocated to combatting crisis and help federating the Community of Interest (CoI) amongst CSDP entities.

Based on a stocktaking of the existing system, the research is expected to focus on the definition of services, interfaces, formats and protocols for sharing selected objects of relevance consumed or produced by the CSDP entities. The research is also expected to focus on interoperable, secure, resilient communication services to be deployed and shared by the involved CDSP entities.

Expected impact:

The research should lead to the creation of a strong community of interest. Additionally, the selected proposal should pave the way of a demonstrator, which should be entirely focussed on the needs of the end-users.

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014

23. Communication technologies and interoperability topic 2: interoperable next generation of broadband radio communication system for public safety and security - PCP[13]

Specific challenge:

Until now each EU Member State has adopted its own radio-communication system for the use of its security forces (Police, first responders, etc.). These are based on similar standards. Unfortunately, most of these systems are not EU interoperable at least from an operational point of view. The EU has already funded a number of research projects to help to overcome this issue. The main challenge is now to make a further step and to push both standardization of Public Protection and Disaster Relief (PPDR) related broadband radio technology and the research done to the institutional market. This will lead to the introduction of innovative, interoperable and cost efficient PPDR broadband communication systems, while preserving the investment done on the currently deployed systems.

The proposed project should take into account the extensive works done so far by other research projects in the field, both in terms of user requirements and of technological solutions proposed.

Scope:

The proposed project must be structured around six different phases, some of which may run in parallel.

1) Technology review and specifications definition

In its initial phase the project will assess lessons learnt from the narrow band TETRA-/TETRAPOL networks, the on-going standardization of PPDR related broadband radio technology, commercially available broadband technology and the technology developed by various EU-wide or national projects in this area, including 3GPP standardization and EU funding works for 5G, due to be based on software defined radio technology, so as to benefit from dynamic ecosystem with significant market size and to ease interoperability. On this basis, the specifications for the next generation of an EU interoperable radio communication system will be agreed upon and become a standard to be used in subsequent steps. All components of the system should be defined, including the network (base stations, network management, including end to end security and handsets. In order to allow roaming and common voice and data communications, the security issues (shared protocols and key management, must alos be determined. The assessment should

[13] For further information please consult Security Research and Industry reference documents available at http://ec.europa.eu/enterprise/policies/security/documents/index_en.htm.

specifically comprise of:

- Identifying and analyzing common communications requirements of PPDR, but also Critical Infrastructure Services, like Transport (Road/Rail/Air/Water), Utilities (Energy, Gas, Water, ..); Telecom operators
- Identifying and analyzing special communications requirements for critical incidents (events/disasters)
- Identifying and analyzing gaps and pitfalls in cooperation between the respective organizations on a national, Europe wide and international perspective

2) Definition of the procurement initiation

In this phase, the project will develop the core text of the specifications to be used as a toolkit to build a basis for national procurement initiation taking into account the EU common requirement for interoperable next generation PPDR broadband communication systems.

3) Definition of the Validation Centre

In this phase, the project will prepare the specifications for a common EU Validation Centre to validate the next generation PPDR radio-communication technology developed during the procurement phase for the next generation PPDR radio communication system.

5) Establishment of the Validation Centre

In this phase the project will contribute, to establish the Validation Centre according to the specifications laid out in the previous phase. Sustainability of the Validation Centre beyond the lifetime of the project should be addressed, both with respect to its legal status and its funding sources.

6) Testing and validation

In the last phase the project will launch a number of interoperability tests for voluntary countries. These should involve multiple first responder and police agencies from at least seven Member States in a cross- border operational setup.

<u>Expected impact:</u>

To create an EU interoperable broadband radio communication system for public safety and security over the next 15 years.

<u>Form of funding:</u>

Programme co-fund - Pre Commercial Procurement (70%)

Specific conditions related to this topic are provided along with the conditions for PCP projects in Annex XX [currently being prepared by DG CNECT].

Specific call year:
This topic is part of the call for 2014

Additional condition:
Proposals should involve multiple first responder and police agencies from at least seven Member States in a cross- border operational setup in phase 1 and phase 6 of the project.

24. Communication technologies and interoperability topic 3: Next generation emergency services

Specific challenge:

The manner in which emergency calls are being made today is changing and the change of pace has legal ramifications for our citizens. Society is using internet-based tools for every day activities (e.g. Skype) but making an emergency call using Skype is not possible. Smartphone penetration is growing rapidly and whilst society benefits from this digital world, the future of how we make emergency calls is not so clear. In this context, there is a need to identify the main requirements of emergency services (the demand side) on the basis of existing research information and to identify research gaps. There is also a need to improve the security of citizens, including those with disabilities or special needs, by creating the environment and infrastructure to allow technology and solution providers (the supply side), in particular SMEs, to test their Internet Protocol-based 112 products end-to-end against such requirements with each other and with the emergency services.

Scope:

The project should contribute to the development of a testing regime for Next Generation 112 products (simultaneous use of voice, data, video and text communications using 112) in a controlled-environment, ensuring that any existing early warning systems for warning citizens of impending disasters/emergencies are future-proofed and interoperable with the NG112 suite of requirements. It should also build a validation-focused programme using existing standards and protocols, with consideration of e.g. call location and routing, video calling to assist people with disabilities, security, integration of social media channels etc. The consortium should gather European technology providers, emergency services organisations, research and development laboratories, telecommunication network providers, Voice Over IP providers, National Regulatory Authorities (NRAs) and software providers to build on the expertise in a collaborative fashion.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

A greater efficiency from emergency service organisations will have obvious societal benefits for all citizens, with a direct positive impact for those citizens with disabilities. This project shall contribute to the implementation of a common standard of emergency call services throughout Europe, ensuring, that the future media for daily communication can also be used for emergency calling. It shall facilitate the interoperability of the many involved technologies and services and their vendors and providers.

Proposed instrument:
Collaborative project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2014

Ethical/Societal Dimension

25. Ethical/Societal Dimension topic 1: Improving protection of Critical infrastructures from insider threats

Specific Challenge:

Critical Infrastructures are crucial assets for the functioning of a society and an economy. Consequently, they can be the target of several threats, in particular terrorist threats.

In this framework, the risk of an insider threat coming from personnel and third party individuals, who have inside knowledge about the infrastructure security practices and/or have access rights to certain key components, data and computer, is particularly high for Critical Infrastructures.

A particular type of insider threat is the one brought along by personnel who have undergone a violent radicalisation process and, as a consequence of that, intend to affect the normal functioning of the infrastructure or, even, to sabotage it.

In order to prevent the latter, it is important to deepen the current knowledge about the main constituents of the violent radicalisation processes to timely detect them and to prevent resulting insider threats to materialize.

Scope:

Research in this area should focus on determining and analysing the main constituent factors of a violent radicalisation process (including family and social environment, psychological factors, religion and ideology, the internet and social media, socio-economic and political factors) as well as on the conditions that can lead a person from ideas to violent action. The proposed actions should take into consideration past and on-going EU research in this field and include, to the extent possible, real life examples of individuals that underwent a violent radicalisation process.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

Expected impact:

The output of this research should be directly applicable to support national and local security practitioners to strengthen the protection of national and European Critical Infrastructures from insider threats brought by violent radicals.

In particular, the research results are expected to contribute to shade light on the violent radicalisation processes and paths and to raise the awareness of the security practitioners about the possible early indicators that can allow a timely detection of insider threats brought by violent radicalised individuals.

The development and application of new equipment and systems to support the security practitioners should also be considered by the proposed research.

The research and the usable results should consider fundamental rights protection, comparative studies of international laws, ethical and societal impacts, with particular consideration for EU anti-terrorism and Critical Infrastructure Protection (CIP) policies.

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014.

26. Ethical/Societal Dimension topic 2: Better understanding the links between culture and disasters

Specific challenge:

Culture is the characteristics of a particular group of people, defined by everything from a set of values, history, language, religion to cuisine, social habits or music and arts. Preparedness, response to disasters and after-crisis recovery is always influenced by cultural background of individuals and the society they live in.

To this end, cultural factors play also an important role in determining the way people respond to stress and accept disaster relief in an emergency situation. At the same time lack of cultural understanding, sensitivity and competencies can hamper and even harm the professional response to disaster as it is crucial to understand the cultural background of disaster victims.

Considering the significance of cultural influences during a disaster especially in urban areas which become more and more diversified, will help increase the effectiveness of all who respond to disasters, will be of value for policy makers and health professionals working in the areas of disaster management or crisis intervention and consequently will help build a more resilient society by ensuring that cities are better prepared for and able to recover from emergencies.

Scope:

Research in this field may focus on the following issues:

- Which cultural factors, important insights, specific communication styles for a given cultural group should be taken into consideration during disaster situations in urban areas?
- How to anticipate and identify solutions to cultural problems that may arise in the event of an emergency?

Proposers are encouraged to analyse how emotional, psychological and social needs, as well as communal strengths and coping skills that arise in disasters can affect the way certain urban communities prepare, respond and recover from disaster.

Expected impact:

This support action will help in better understanding the links between disaster and culture in urban areas. The research and its results will serve as input to build necessary strategies meeting the needs of various cultures in order to provide disaster relief.

Last but not least, taking into account past and on-going EU research, this project will provide a framework for improving disasters' policies and practices by taking into consideration every disaster victim's cultural and personal uniqueness with a view to contribute to building a more resilient society.

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014

27. Ethical/Societal Dimension topic 3: Impact of climate change in third countries on Europe's security

Specific challenge:

Climate change in Third Countries is a real threat to security of the European Union. Extreme weather or other climate events which devastate lives, infrastructure, but also institutions and budgets can have disastrous consequences on European security, as climate-driven crises occurring outside the EU can have detrimental effects and direct or indirect security implications on the Union (e.g. climate-driven migration forcing large number of people to move from their homelands to another country – EU Member State; supply chain security; food security; reliance on imports of raw material etc.), including EU assets in third countries.

Therefore, adequate political, strategic and institutional responses should be found in order to enhance international and European cooperation on the detection assessment and monitoring of the security threats in Europe related to climate change in other regions of the world. European policy makers and analysts as well as national governments should tackle climate change as today's non-traditional security hazard.

The research and consecutive execution of the project has as its aim facilitating the adoption of a comprehensive approach, which will provide a way to consider risks and vulnerabilities in order to take necessary steps to give more attention to the impact of climate change on security and at the same time will help minimise negative consequences of climate-driven crises.

Scope:

Research in this field may focus on the following issues:

- What kind of instruments, tools, and actions can be used alongside mitigation and adaptation policies to address the climate change security risks?
- Which could be the most efficient ways of developing contingency plans for the EU's response to the effects of climate-driven crises occurring outside the Union that have direct or indirect security implications on the Union?

Expected impact:

This action will help to better understand consequences of climate change events in Third Countries on security implications in the EU.

Taking into account past and on-going EU research, this topic should thoroughly examine the impact of climate-driven crises on European security in order to provide a framework for improving situation analysis and policy planning at the EU level.

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2014

Conditions for this call

Publication date: 25 March 2014 [TBC – the dates for the 2015 call are not yet clear]
Deadline: 28 August 2014 at 17:00 hours Central European Time [TBC – the dates for the 2015 call are not yet clear]

Indicative budget: [Budgetary indications are not yet possible, due to the lack of agreement in the trilogues on the overall budget of Challenge 7]

Option 1: Indicative budget : EUR XXX million from the *[Insert year e.g. 2014 or 2015, in some cases both years could be mentioned]* budget

	2014 EUR million	*2015* *EUR million*	
Topics: 2, 4, 5, 7, 8, 9, 11, 12, 13, 14, 21, 22, 23, 24, 25, 26, 27	TBC	-------------------	*All single stage*
Topics: 1, 3, 6, 10, 15, 16, 17, 18, 19, 20	-------------------	TBC	*All single stage*

Eligibility conditions:

The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Topics 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 28, 19, 20, 21, 22, 24, 25, 26, 27	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.
Topic 5	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.
	At least 3 Member States relevant public authorities
Topic 23	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.
	Proposals should involve multiple first responder and police agencies from at least seven Member States in a cross- border operational setup in phase 1 and phase 6 of the project.
	Specific conditions related to this topic are provided along with the conditions for PCP projects in Annex XX [currently being prepared by

	DG CNECT].

Evaluation criteria:

The standard evaluation criteria apply. Please read carefully the provisions [*Link to the annex on standard evaluation criteria*] under Annex X before the preparation of your application.

Evaluation procedure: [*Link to the annex on standard evaluation procedure*]

- Proposal page limits and layout: 120 pages [TBC]
- Indicative timetable for evaluation and grant agreement[14]: *[as appropriate]*
  - *specify planned date to inform applicants of outcome of evaluation, and.*
  - *indicative date of signature of grant agreements or notification of grant decision*

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements
Topics: : 2, 4, 5, 7, 8, 9, 11, 12, 13, 14, 21, 22, 23, 24, 25, 26, 27	15/12/2014	15/03/2015
Topics: 1, 3, 6, 10, 15, 16, 17, 18, 19, 20	TBC	TBC

Consortia agreements: *[as appropriate]*

[Standard sentence on climate change and/or sustainable development *[to be added as necessary]*

[14] Should the call publication postponed, the dates in this table should be adjusted accordingly.

Border security

Contents

With the Lisbon Treaty in force the EU is better placed to exploit synergies between border management policies on persons and goods, in a spirit of solidarity and sharing of responsibilities. In relation to movement of persons the EU treats migration management and the fight against crime as twin objectives of its integrated border management strategy. Technologies and capabilities are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security, including both control and surveillance issues, exploiting the full potential of EUROSUR and promoting an enhanced use of new technology for border checks, also in relation to the SMART BORDERS legislative initiative. In relation to the movement of goods the 'security amendment' of the Community Customs Code lays down the basis for the border to become safer and yet more open for trade of trusted goods. Technological solutions will be developed and tested considering their effectiveness, compliance with legal and ethical principles, proportionality, social acceptability and the respect of fundamental rights.

This call does not foresee any topic on land border surveillance because a specific POV on land borders is to start early in 204. The topics proposed for the surveillance of the maritime domain correspond to the two challenges identified by ESRIF:

1. Reduce the loss of human life related to trafficking in human beings and illegal migration activities by sea,
2. Fight against unlawful and criminal activities at sea (e.g. drug smuggling via low flying aircraft)

The identified challenges relevant to checks at border crossing points are primarily to prohibit unwanted activities, while facilitating the large volume of legitimate border crossings. Effective and efficient checks at the border of people and goods require a broad range of solutions. Some devices are better for checking people, others for cargo.

Maritime Border Security

1. Maritime Border Security topic 1: radar systems for the surveillance of coastal and pre-frontier areas and in support of search and rescue operations

Specific challenge:

The challenge refers to early and long distance border surveillance. Research is needed in the development of surface wave and sky wave Over the Horizon (OTH) radars of improved performance, reduced cost, lower power requirements, deployable. These technologies are expected to be appropriate to support Search-and-Rescue (SAR) operations in the Mediterranean Sea.

Scope:

Pre-competitive research is expected to involve the various stages of development, from sensor design, to the analysis and design of system configuration and integration and validation by (public) authorities for target detection, identification and recognition. Projects will focus only on border surveillance and search and rescue (not defence) needs. A validation work package should therefore be foreseen in a realistic SAR operational scenario.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

This topic would contribute further to the development of the European Border Surveillance System (EUROSUR). HF technology provides extended coverage over the coastal marine band radars, potentially reaching pre frontier detection, thus proving appropriate for the three main missions of EUROSUR, particularly the third which refers to the reduction of the current death toll at high seas through the extension of SAR capability in a flexible way.

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding:

Collaborative Project 70% funding (Capability Project)

Specific call year:

This topic is part of the call for 2014.

2. Maritime Border Security topic 2: Low cost and “green” technologies for EU coastal border surveillance

Specific challenge:

The use of low cost and “green” technologies is expected to become mandatory for future border control systems in environmentally sensitive areas. Systems of passive (or low emission) radar technologies provide promising results for the detection of targets in areas that cannot be covered by active systems. Passive radars offer different advantages, such as lower detectability and cost and the possibility of use practically anywhere.
R&D is needed to better apply this technology to the environment of maritime surveillance, also in combination with other systems, and using the signals coming from existing coastal systems.

Scope:

The areas of research and development are expected to include, among others:

1. further development of devices and sensors for maritime targets and environment (e.g. fit for mobile platforms)
2. development of specific tracking and fusion algorithms
3. operation in network configurations together with other systems for improved performances

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

This topic would contribute further to the development of the European Border Surveillance System (EUROSUR).

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding:
Collaborative Project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2015

3 Maritime Border Security topic 3: Light optionally piloted vehicles for maritime surveillance

Specific challenge:

Beyond coastal waters, surveillance tools such as Off-shore Patrol Vessels (OPV) and Maritime Patrol Aircrafts (MPA) are used as mobile assets to identify and position targets. However, MPAs (and helicopters) have very high operational costs, whilst the lack of regulations to fly outside a segregated air space impose limits the utilization of Unmanned Aerial Vehicles for the surveillance of remote areas.

This R&D is therefore targeted to extend the portfolio of light surveillance platforms for reduced operational cost, and increased capability in surveillance in high seas (to be tested in the context of a real operational scenario, such a Frontex led joint operation.

Scope:

The research should cover technologies (e.g. low weight/high performance radar and electro-optic)/systems for the detection and early identification and tracking of moving targets (e.g. with moving target indication and data fusion/correlation capabilities). These technologies could also be useful for the detection of marine pollution incidents.

The fitness for purpose of novel solutions should be validated using affordable platforms (compliant with current regulations) connected with ground control stations, as in legacy surveillance systems.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

This topic would contribute further to the development of development of the Common Information Sharing Environment (CISE) at sea initiative, as included in the final steps of the European Border Surveillance System (EUROSUR).

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs. These technologies developed could, in addition, also be used to support the detection of marine pollution incidents.

Form of funding:
Collaborative Project 70% funding (Capability Project)

Specific call year:
This topic is part of the call for 2014.

4. Maritime Border Security topic 4: Detection of low flying aircraft at near shore air space

Specific challenge:

The deployment of maritime surveillance system for border control has exerted pressure on smugglers in the last years. Drug smugglers reacted by changing their modus operandi using low flying aircrafts to cross borders undetected. As an example, this situation has been identified as a major gap to combat drug smuggling entering through the south coast of Spain.

In this case the typical scenario (in line with the concepts of operations being defined by the Frontex agency) is a small low flying aircraft loaded with drugs coming from the North Mediterranean coast of Africa and entering southern European coasts. This kind of aircrafts land in small airports or runways. Landing areas are well known by security forces. Nevertheless, the early detection of these aircrafts is crucial to determine the landing area.

Scope:

Required technologies and systems to be investigated and developed may include:

1. Mobile units which can be quickly deployable in remote areas with communication links with command and control centres.
2. Multi-mode radar technologies for the early detection and tracking of low flying aircrafts.
3. Integration of radar data and correlation with repositories of information to predict most probable landing areas.

The scope and outcomes of this line of research may be applied also to land border security.

Solutions should be validated in a realistic operational context.

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

This topic would contribute further to the development of the European Border Surveillance

System (EUROSUR)

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding:
Collaborative Project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2015.

Border crossing points

5. Border crossing points topic 1: Novel mobility concepts for land border security

Specific challenge:

Border authorities are facing new challenges to secure land borders of the EU/Schengen areas, while the recent trends show a significant increase of travellers' flows. In the meantime, travellers are requiring fast and convenient border crossing, therefore pushing authorities to implement novel approaches in order to maintain and even improve the throughput at the crossing points.

Infrastructure for land border checks is not very flexible. As a consequence, improved solutions are required. They could rely on the development of mobility concepts along with traveller programmes that are extensively being developed in order to facilitate border crossing. Moreover, the current wide-spread use of mobile devices such as smartphones or tablets provide potentially exploitable means and distributed Computer Processing Units (CPU) power that could (or could not) be combined with border authorities dedicated mobile equipment to perform identity checking for border security.

Scope:

Research should lead to novel mobility concepts for land border security enabling authorities to achieve higher throughput at the crossing points whilst guaranteeing high security level, enabling fast processing of passengers within vehicles or pedestrians and improving the efficiency of passengers flow management. In particular, the use of passengers' personal mobile devices is expected to enable efficient and reliable identity checks through the application of biometric technology. The ability to automatically detect document forgeries is also expected for further improvements. Projects should therefore aim at proposing novel concepts relying on the use of traveller's personal mobile devices and/or border authorities' specific mobile equipment for high security level passengers' identity control. What is needed is to perform biometric identification of travellers inside vehicles (cars, bus trains) as well as pedestrians. R&D could propose novel technological solutions as well as procedures to manage relevant associated workflows (to be validated by border guards in a realistic operational scenario). An appropriate portable (and, if seemed necessary, fixed) ABC gate for land borders could be developed (if portable, this gate should be movable so that it could be used at lanes outside the terminal). In this research legal, ethical or social implications must be taken into account appropriately.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross-border flows of people (and goods).Border control is likely to face increasing demands for efficiency, which implies a need for technical systems that are user friendly and reliable in operational conditions. A general challenge is to make the technical equipment affordable enough to be widely employed. The approach to use technology from adjacent markets such as mobile telecommunications where the volumes of production are very high could help the costs of processing down to a minimum. Harmonization of requirements across Member States (and standardization) is expected to also automatically greatly improve affordability.

Form of funding:

Collaborative Project 100% funding (Capability Project)

Specific call year:

This topic is part of the call for 2014.

6. Border crossing points topic 2: Exploring new modalities in biometric-based border checks

Specific challenge:

The ever-growing number of travellers crossing the EU borders poses a serious challenge to the border control authorities in terms of a reduced amount of time for carrying out border checks. Consequently, efforts have already been undertaken to facilitate the travel of bona-fide and genuine passengers and simultaneously to safeguard high level of security. In particular, in the field of person and document authentication and/or verification deployment of biometric-based approaches led to significant advances as regards making the border control processes more efficient. Further explorations going beyond state-of-the-art biometric-based person identification detection techniques are expected to contribute to making the daily work of border control authorities more efficient and to significantly facilitating non-EU citizens in crossing EU external borders.

Scope:

Research is needed in order to explore whether it is possible to use other biometric data (potentially already used in another context and in another domain) than fingerprint, iris or picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and can be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. For instance the feasibility of storing DNA string or behavioural biometrics in the e-Passport could be explored. In addition, practical experiences lead to the assumption that for non-critical travelers (EU, bona-fide etc.) a most fluent non-intrusive control process is desired. Therefore, to increase accuracy, in this case the use of contactless techniques (e.g. face, 3D face, iris) and multi-biometric fusion is likely to be preferred over contact-based technologies.

While the introduction of new biometric-based modalities in the process of person identification might lead to making this process more accurate and efficient, an integral part of the research should also embrace related ethical, societal and data protection aspects. Work should include optimization of the use of current biometric modalities and consideration of how services offered by countries outside of the EU may result in a more efficient and user-friendly experience for the traveler. Development of modeling techniques and the creation of datasets for use by academics and commercial entities should be a priority. The work carried out should also include research on the theme of multi-modal biometrics in border control.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Non-EU residents contributed €271 billion to the economy of Member States when travelling to the EU in 2011. Business travellers, workers, researchers and students, third country nationals with family ties to EU citizens or living in regions bordering the EU are all likely to cross the borders several times a year. Making it as easy as possible for them to come to the EU would ensure that Europe remains an attractive destination and helps boosting economic activity and job creation.

Form of funding:
Collaborative Project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2015.

7. Border crossing points topic 3: Improving border checks at railway Border Crossing Points

Specific challenge:

Border Control authorities are facing various new challenges resulting from an ever-growing number of travellers crossing the EU borders. In particular, it has been acknowledged that carrying out border checks at railway Border Crossing Points (BCP) poses problems in terms of very limited time for processing and retrieving information related to a person being checked and the specific conditions in which checks are carried out (movement of the train over long distance) which impacts the performance. Although mobile document readers are already on the market and are being successfully deployed on trains, the entire border check process at railway BCP and on trains might and often does require retrieving information from numerous information systems, not necessarily available at hand, and whose obtaining is time critical.

Scope:

Research is needed in order to explore new technical solutions that could allow carrying out border checks at railway BCPs and on the trains in a more efficient manner, while preserving a high level of security and privacy. In particular, elaboration of a concept, development and testing of ”all-in-one” mobile terminal that could reduce the information processing and retrieval time should be undertaken. The potential solution should be highly flexible, namely, it should not only take into account all related existing and emerging national and EU-level information systems (e.g., EES), but also integration/linking to future systems. Similar-in-nature scenarios to railway BCPs could be considered too.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Non-EU residents contributed €271 billion to the economy of the Member States when travelling to the EU in 2011. Business travellers, workers, researchers and students, third country nationals with family ties to EU citizens or living in regions bordering the EU are all likely to cross the borders several times a year. Making it as easy as possible for them to come to the EU would ensure that Europe remains an attractive destination and help boosting economic activity and job creation.

Form of funding:
Collaborative Project (100%) - (Capability Project)

Specific call year:
This topic is part of the call for 2014.

8. Border crossing points topic 4: Optimization of border control processes and planning

Specific challenge:

Apart from the known problem of a continuous increase of travellers crossing EU external borders border control authorities are confronted with a wide range of other problems, including: (a) less staff and financial means in the nearby future, (b) emergence of new technologies that are supposed to support border control authorities in carrying out border control and surveillance tasks, and (c) an ever-growing amount of information available to them coming from various sources (e.g., national or international information systems, sensors, open sources, etc.). Having "less people", but "new tools and machines" and "more information available" requires establishment of mechanisms to improve decision making processes in the context of planning resources allocation and information workflows.

Scope:

Research is needed in order to conceptualize and develop tools that would facilitate: (a) planning cost- and performance-efficient allocation of assets and human resources to border control tasks, (b) exploration of how to best combine humans with new technologies (e.g., through simulations, virtual environments), and (c) designing optimal information workflows for particular border control scenarios, i.e., which information to utilize and fuse with other, and which to discard, etc. The underlying data to support the decision making and/or planning in the context of such tool could come from the information gathered over longer period of time from the past.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross border flow of people and goods. Border controls thus face increasing demand for efficiency, which implies the need for technical systems that are user friendly and reliable in operational conditions. A general challenge is to make the equipment and procedures appropriate for wide employment. A further general challenge that applies to all scenarios is interoperability (operational as well as technical).

Form of funding:
Coordination and Support Action 100% funding

Specific call year:
This topic is part of the call for 2015.

9. Supply Chain Security topic 1: Development of an enhanced non-intrusive (stand-off) scanner

Specific challenge:

Smugglers try to evade controls at borders by using their bodies as the conduit to conceal prohibited or restricted goods. These items will be narcotics, explosives, currency and weapons and could be ampoules containing chemical and biological threats. All could remain undetected by conventional technologies.

There is a need to develop body-scan technology able to discern those commodities sought by Customs, from benign materials carried by travellers. The device/system should have the capability to automatically identify the chemical composition of the main threat commodities. Such systems will improve efficiency of inspection of suspected individuals, improve security at the border and act as a deterrent to other potential smugglers.

Scope:

There are two different scenarios that technology is required for. Although ideally a system would have a capability to be deployed to cover both operational situations, it is accepted that at this stage it may not be possible, due to the types of core technology used, so within this topic the requirements are shown separately to clarify challenge and so assist development in that proposals may be for either sub category or a combined solution.

1) Internally concealed commodities

Packages such as drugs, may be ingested, or inserted into body orifices. Ingested packages may be formed of compressed powder, or even liquid and may be from a few hundred grams up to over a kilo. Non-ingested items may be several hundred grams. Drugs, used in the example, are by nature organic, so it is difficult to distinguish them visually from other organic or food waste in the digestive system of the human body. Transmission x-ray is a useful tool, but it is an imaging technology which requires interpretation. There is a potential for error and packages may be missed.

There is a requirement to develop a body-scanner capable of identifying and alerting an operator to specific threats such as narcotics /explosives etc concealed inside the body. If the technology in the proposal utilises ionising radiation, it would have to comply with European limits of dose. It should also be noted that not all member states permit use of ionising radiation for non-medical purposes.

2) Externally concealed commodities.

Packages such as drugs can be concealed beneath clothing and even moulded to map the body contours, which can be compensated for by the wearing or larger clothing. A human can conceal up to 5 kilos in this manner, which can be remain undetected. Millimetre wave technology offers some potential for detection; however these are only anomaly detectors and cannot distinguish between threat and benign materials. Organic materials which have been on the body for a significant duration can become opaque to some technologies if they are close to the body temperature. The ideal novel solutions must be able to distinguish those materials of Customs interest from harmless items and alert the operator to this and this solution would typically be applied to a "non-divest" situation. It must be able to work in real-time, not to disrupt passenger flow or movement of a crowd. Preferably the solution should be able to deal with more than one person within the field of view, or at least other people in the frame should not interfere with the performance of the primary target. Performance will have to be validated in a realistic scenario.

The technology should pose no risk to particular groups, or those with health issues (children, pregnant woman, pacemakers) Privacy of individuals *must* be respected.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

The technology to be developed under (1) and (2) would be operated by Customs/Border control staff and is expected to exceed the capability of current technologies being used by Customs administrations in some member states. If the appropriate capability is developed, it is expected to significantly improve security at the border and will constitute an effective tool against organised crime..

Form of funding:
Collaborative Project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2015.

10. Supply Chain Security topic 2: Technologies for inspections of large volume freight

Specific challenge:
Approximately 70% of all cargo is transported in intermodal shipping containers representing

approximately 240 million container moves in any given year. As a major trans-shipment hub,

the EU handles around a third of the container moves throughout the world. Container security associated with terrorist threats, illegal immigration, theft and smuggling is therefore an

important factor in the overall EU border security.
Customs currently employ a limited amount of technology to assist in working on its largest problem: how to counter hiding/smuggling in large volume freight. Thus far the technology of choice is X-ray interrogation (supported by risk-selection). Ideally, upon effective risk selection, the most effective (array of) technology out of a number of availabilities should be selected to screen the freight. The best results (relative low false-positive, relative low false negative) is expected to be achieved in a situation in which (at least) two independent technologies are employed in conjunction

Scope:

The research should explore options for parallel development of at least two different technologies for container scanning:

1) Atomic property based interrogation (e.g. X-ray, muon, neutron), particularly to detect threat materials shielded in dense cargos, interrogation technology being directed towards the detection of organic products of relevance to Customs;

2) Evaporation based interrogation (e.g. mass spectrometry, biological detection, ion mobility spectrometry), with targeted selectivity at approximately femtogram/ litre level, to be directed towards a wider scope.

These combined approaches should be validated in an operational scenario, to come up with practical, wide scope, detection tool to be used on large volume freight (e.g. containers and large pallets).

Projects addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive foreground information. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that projects requesting a contribution from the EU of between €5m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

This topic should look for an enhanced international cooperation, through a recommended participation of International Cooperation (INCO) partners, following current discussions and workshops with relevant international research partners, and in particular with US homeland security research entities.

Expected impact:

The research is expected to provide a substantial contribution in the prevention of the unlawful transport of dangerous and illicit materials, also protecting critical elements of the supply chain from attacks and disruptions. The greatest volume (and risk) of illegal/illicit/mis-declared goods into the EU, as of interest to Customs, include, but are not limited to: illicit narcotics (heroin, cocaine, etc.) explosives, tobacco products, chemicals. Intelligence together with scanning is useful in narrowing suspicious consignments, but ultimately a physical examination of the load is required. This is resource intensive and adds cost and delay to importers, should the anomaly be found to be benign. A technology which could scan a load with high probability of detection of particular key commodities would increase efficiency and throughput and reduce cost and delays to innocent shippers. Solutions are therefore to be developed to allow for an increased assurance level in particular for dense containerised cargo, avoiding the need to unnecessarily resorting to physical inspection. It is difficult to predict a priori which technology will yield the most practical solution. This will have to be validated in a realistic scenario. As the research should facilitate and expedite the smooth flow of legitimate international trade through improved security controls, it would the work of WCO for high risk cargo.

Form of funding:
Collaborative Project 100% funding (Integrated project)

Specific call year:
This topic is part of the call for 2014.

Ethical Societal Dimension

11. Ethical Societal Dimension topic 1: Human factors in border control

Specific challenge:

Border control relies on a number of presumed abilities in those performing it. These include the ability to:

- stay alert from the beginning of a shift to the end;
- distinguish truth from falsity;
- detect malicious intent;
- detect invalid or falsified documents;
- detect hidden goods or humans in vehicles;
- detect behavioural indicators of persons engaged in, or methods used to undertake, illicit activity.

Scope: The project should list and carefully analyze the psychological factors which may affect the performance of key border guard tasks and also include a review of the psychological literature relevant to such task. It should suggest remedies and a strategy for improving performance at them (whether improving human performance), in this way making a major contribution to the effectiveness of EU border control. The research should help to identify which tasks related to border control could be carried out in a more automated manner, and for which tasks the human factor is indispensable.

The Commission considers that projects requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross-border flows. Border control is likely to face increasing demands for efficiency, which implies a need for technical systems that are user friendly and reliable in operational conditions. This research would contribute to the implementation of the Smart borders initiative (and future regulation) , reinforcing checks while speeding up border crossing for regular travellers, optimizing procedures and enhancing the security at the moment of the crossing of the EU external borders.

Form of funding:

Collaborative Project 100% funding (Capability Project)

Specific call year:
This topic is part of the call for 2014.

CONDITIONS FOR THIS CALL

Publication date: 25 March 2014 [TBC – the dates for the 2015 call are not yet clear]
Deadline: 28 August 2014 at 17:00 hours Central European Time [TBC – the dates for the 2015 call are not yet clear]

Indicative budget: [Budgetary indications are not yet possible, due to the lack of agreement in the trilogues on the overall budget of Challenge 7]

Option 1: Indicative budget : EUR XXX million from the *[Insert year e.g. 2014 or 2015, in some cases both years could be mentioned]* budget

	2014 EUR million	*2015* *EUR million*	
Topics: 1, 3, 5, 7, 10, 11	TBC	-------------------	*All single stage*
Topics: 2, 4, 6, 8, 9	-------------------	TBC	*All single stage*

Eligibility conditions:

The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Topics 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Evaluation criteria:

The standard evaluation criteria apply. Please read carefully the provisions [*Link to the annex on standard evaluation criteria*] under Annex X before the preparation of your application.

Evaluation procedure: [*Link to the annex on standard evaluation procedure*]

- Proposal page limits and layout: 120 pages [TBC]
- Indicative timetable for evaluation and grant agreement[15]: *[as appropriate]*

- specify planned date to inform applicants of outcome of evaluation, and.
- indicative date of signature of grant agreements or notification of grant decision

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements
Topics: 1, 3, 5, 7, 10, 11	15/12/2014	15/03/2015
Topics: 2, 4, 6, 8, 9	TBC	TBC

Consortia agreements: *[as appropriate]*

[Standard sentence on climate change and/or sustainable development *[to be added as necessary]*

[15] Should the call publication postponed, the dates in this table should be adjusted accordingly.

Cybersecurity and Privacy

Contents

The European Strategy for Cybersecurity highlights a set of actions to be implemented by the European Commission to "…develop the industrial and technological resources for cybersecurity…", "… promoting a Single Market for cybersecurity products…", and "… fostering R&D investments…". This call will be one of the instrument to reach these aims.

Cyber-security is a multi-faceted issue (involving critical economic and civilian stakes; cybercrime; defence; human rights protection; norms of behaviour). The proposed activities in this domain address the economic and societal dimension of security in the digital ecosystem, for the purposes of ensuring the well-functioning of the internal market. This work contributes to the efforts being done in the other areas relevant to cyber-security.

Securing the digital society must be our central concern. It entails preventing cyber-attacks on any component of the digital society (networks, access devices, IT services, ….) no matter what their nature or origin; as well as protecting physical (e.g. critical infrastructures) or intangible assets (e.g. finances, intellectual property, privacy). As a consequence this call addresses the technology to secure the infrastructure (e.g. networks), hardware (e.g. access devices), services (e.g. cloud computing), components (e.g. RFID), software (e.g. operating systems, web-browsers), etc… against accidental or malevolent use. As cybersecurity is cross-domain the call will provide cybersecurity whatever the application or domain (mobile, eCommerce…), or societal challenge (e.g. health, energy, smart cities, …).

This Objective will thus focus on demonstrating the viability and maturity of state-of-the-art security solutions with the intention that after this validation phase they will find a wide up take in the market. Proving that the security concepts, processes and solutions work in a real life environment, in large scale demonstrators and directly involving end users who would ultimately benefit the most from the outcome, should increase the prospects for an ICT security market and demonstrate the validity and effectiveness of security. This in turn will reduce the risks of a negative economic impact due to a cyber-incident.

This call is complementary to activities supported under the "Information and Communnication (ICT)' theme of the 'Leadership in Enabling and Industrial Technologies' (LEIT) pillar of H2020. Work in LEIT will address both prospective research on cybersecurity for the next generation of ICT and the technology gaps identified by the Societal Challenges actions.

1. Privacy

Specific challenge:

Privacy is a major concern for online users. An overwhelming majority of online users is reluctant to disclose personal information online because of privacy concerns. Personal data has become an economic asset, but it is not the owners, i.e. the users, that control or monetize it. This is in the hands of the service providers whose business case is often built on the exploitation of the personal data they collect (e.g. social networks, search engines, online retailers, cloud hosting services).

Therefore, despite the existence of a data protection and privacy framework in Europe service providers are reluctant to respect the rules or implement them in a user-friendly way as this would harm their business case. There is also a lack of enforcement of the rules. As a consequence, users have either no choice, or difficulties in exercising their rights. Either way, users are deprived of the economic benefit derived from - the exploitation of their personal data. As the economic value of their data is obscured, users are not able to evaluate the value of their data relative to the value they assign to a "free" service. That indicates a market failure. Moreover, the user has no control over what happens with his data, e.g. he cannot verify the data is not passed on to 3rd parties.

Scope:

The focus is on the development of solutions to protect individuals' privacy by default while empowering the users to themselves set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving him control over how his data will be used by service providers, and making it easier for them to verify both whether their online rights are respected and if they get a reasonable bargain. Systems will either have to automatically detect the privacy settings, or the data will have its privacy settings permanently associated to it by the user.

Activities can include the investigation of preventive measures to safeguard privacy in the context of mass data handling, for example for services exploiting big data, cloud services, data sharing by interconnected devices in the internet of things, and data handling in the highly sensitive context of criminal investigations.

Where relevant, actions can be proposed to apply privacy-by-design frameworks for a range of different applications to promote the usage of privacy enhanced technology.

Expected impact:

Support the practical implementation of the legal obligation for prior consent; the identification and implementation of privacy by design architectures. Increased user trust online. Generate positive business cases for online privacy.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2014

2. Access Control

Specific challenge:

Security includes granting access only to the people that are entitled to it. Currently the most widespread approach relies on passwords. Managing the passwords has its limits and poses a challenge to the user, which adds additional vulnerabilities. Common practice is to use the same or similar password, which increases significantly the risk should the password be broken.

Scope:

The focus is on the development and testing of usable, economic and privacy preserving access control platforms based on the use of biometrics, smart cards, or other devices. The solutions are to be installed and tested in a broad band network, giving access to smart services running over networks with state-of-the-art security, avoiding single points of failure. Proposed work should include the management of the access rights in particular for the service providers, ensure the security and privacy of the databases, facilitate a timely breach notification and remediation to the user, and reduce the insider threat.

The proposed solutions have to guarantee interoperability and portability between systems and services, sparing the user to have to install a platform, service or country specific technology.

Proposed work could assist the objective of implementing a secure information sharing network.

Expected impact:

User-friendly secure access to ICT systems, services and infrastructures. Increased protection of online services and critical infrastrcutures. Consumerisation of devices for access control. Creation of commercial services making use of electronic identification and authentication.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2014

3. Secure Information Sharing

Specific challenge:

A lot can be gained by exchanging information on vulnerabilities, incidents or attacks. For this reason, the proposed Directive on Network and Information Security (NIS) is imposing obligations to share and report information on major incidents and the NIS public-private platform will discuss, among the other things, best practices on information sharing and incident coordination thereby complementing and underpinning the implementation of the Directive. However, at the moment the private sector and the national relevant security authorities are reluctant to share information unless they have a system and counterparts they can fully trust.

A variety of sources of information for incidents or vulnerabilities exist. For example, some business sectors have set-up a sector specific information sharing; large service providers, network operators and antivirus companies monitor attacks and exploits on their infrastructure and on the user systems; CERTs are providing services. However, those sources are rarely integrated or are not interacting by exchanging information between them.

Scope:

This objective goes beyond preserving the confidentiality of a point-to-point communication. It rather encompasses the development and implementation of a network for secure sharing of sensitive information, like a network of NIS competent authorities, law enforcement agencies, business sectors and end users. Where appropriate it will link existing networks and incident sharing platforms, making to the largest extent possible use of existing infrastructures and determine the cooperation mechanisms between industry and public authorities such as EC3, CERT's, law enforcement agencies, etc….

The network should be a multi-layer security network, permitting different levels of access over the same network sharing the relevant information between the different stakeholders with different security requirements. The network should provide additional functionalities like traffic monitoring and analysis, intelligence and trend analysis, managing trust in architectures comprising untrusted components, trust management over the whole data lifecycle, technical support to compromised users (in particular SMEs), automated and secure responses to threats and incidents, decision support to select and engage appropriate counter measures, facilitate the communication of security warnings from public authorities to business (including SMEs) and end-users.

Several pilots will be supported, for different application areas. The selected pilots will have to engage with the NIS platform, contribute to its objectives and take due consideration of its recommendations.

Expected impact:

Operational information sharing between the public and private sector. Building trust between the public and private sectors. Reduced impact of incidents. Increase the level of preparedness of SMEs. Faster response to incidents and/or vulnerability through faster sharing of information and an enlarged source of information.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2015

4. Trust eServices

Specific challenge:

The implementation of trust eServices in specific applications areas like health, public administration, eCommerce includes the provision of electronic signatures, e-seals, timestamps or certified electronic delivery. The deployment and widespread adoption of these eServices is hampered by the lack of globally interoperable solutions, mutually recognized or compatible trust models and the absence of solid business cases for the reliance on electronic signatures, e-seals, timestamps or certified electronic delivery. In addition, the impossibility of transparently assessing the security assurance and trustworthiness of such eServices, in particularly when coming from third countries makes it difficult for citizens and businesses to confidently rely on them.

Scope:

The objective is to devise demonstrators for the automated comparison and interoperability of electronic trust services covering aspects such as security assurance levels, operational security audits, state supervision systems, data protection regimes or liability of trust service providers. Solutions should rely on state-of-the-art technology, interoperability linking existing electronic identification and authentication systems, taking into account different jurisdictions. Key elements of the initiative will be the differential assessment of technical and organisational standards for trust services, as well as the development of a framework for 'global trust lists'.

Validation platforms able to handle the specificities of various jurisdictional or national systems could be created to provide easy to understand assessments of the trustworthiness of any given trust service..

Expected impact:

Demonstrate a positive business case and the economic value for the use of and reliance upon trust eServices. By paving the way for global interoperability of trust eServices, the initiative should contribute to empower and protect users in their digital experiences like e-contracting, e-bidding, e-invoicing or accessing social networks. The initiative should create the conditions for more commercial applications and services to integrate the use of e-signatures, timestamps, e-seals and certified electronic delivery. Enhancing the trustworthiness of electronic transactions will ease the dematerialisation of processes, reduce administrative overhead for citizens and businesses and, last but not least, facilitate higher availability of eGov services.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2015

5. Risk management and assurance models

Specific challenge:

The ability to assess, manage, reduce, mitigate and accept risk is paramount. The dependence of networks and information systems, that are essential for the functioning of our societies and economies (including Critical Infrastructures), on public communication networks and off-the-shelf components is an additional risk. However, in the area of cybersecurity, recent developments and trends render traditional (i.e. static and iterative) risk management methodologies ineffective and rapidly obsolete.

Moreover, the proposed Directive on Network and Information Security will impose risk management obligations for cybersecurity for several business sectors. There are however no generally accepted best practices guidelines for risk management, nor a consensus on the minimal requirements for the market actors concerned, neither at a sectorial, nor at cross-sector level. For this reason, the NIS public-private platform will seek to identify best practices on risk management, including information assurance, risks metrics and awareness raising.

Also, although the NIS Directive does not impose risk management obligations on software developers and hardware manufacturers, it is essential to ensure that a risk management culture is well-established in those components of the value chain.

Scope:

The proposals should implement a pilot to demonstrate the viability and scalability of state-of-the-art risk management frameworks. The risk management framework will have to encompass methods to assess and mitigate the risks in real time. Work should include a socio-economic assessment to evaluate the cost-benefit of implementing the framework. The framework should be dynamic, continuously adapted to new ways of managing risk to keep up with the ever evolving threat and vulnerability landscape. New ways of dealing with the security risk resulting from on-demand composition of services and massive interconnectivity should be developed.

The work on risk management frameworks can be complemented with the development of tools to evaluate the risks and its impact on business, tools for preventive assessment of risk and trustworthiness of customers and providers, tools providing a simple view and understanding of a complex system, and tools to detect social engineering attacks.

Current assurance models and the resulting control and audit frameworks should be revisited. The applicability of the methods to the calculation of insurance premiums should also be investigated.

The selected pilots will have to engage with the NIS platform, contribute to its objectives and take due consideration of its recommendations..

Expected impact:

A risk management framework has to be put in place addressing not only legal requirements (such as imposed by the NIS Directive), but allowing the comprehensive comparison between the sector specific or national approaches, and providing an assessment on the residual risk. Facilitate the implementation of legal obligations on risk management and identify gaps in existing legislation.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2015.

6. The role of ICT in Critical Infrastructure Protection

Specific challenge:

Communication and computing networks are not only critical infrastructures on their own, but underpin many other critical networks (e.g. energy, transport, finance, health …). In addition they are critically dependent on ICT technology. Therefore, the malfunctioning or disruption of the communication channel or of an IT system will have a cascading effect, on several other infrastructures or services that depend on it, potentially across all Europe.

Many vulnerabilities of critical infrastructures, including the communication networks, stem from the fact that ICT systems are deployed in an environment or for an application that it was not designed with security in mind. The deployment of ICT in new critical systems, including new generation ICT system, is exacerbating the problem by constantly introducing new risks and vulnerabilities, in particular for an interconnected system.

Scope:

Proposals should investigate the dependencies on communication networks and ICT components of critical infrastructures, analyzing and mitigating the criticalities, developing tools and processes to monitor the propagation towards the critical infrastructures of an incident occurring in the ICT layer, and develop self-healing mechanisms. ICT should be protected or re-designed at the software level, but also at the physical level, leading to more robust, resilient and survivable ICT infrastructure.

Based on the outcome of the work described above, plans of how to retrofit state-of-the-art security into networks can also be addressed.

The investigated concepts have to be tested in a field trial. Trials will have to distinguish between generic solutions and solutions specific to the critical infrastructure (e.g. health, finance, energy, transport, …) they are applied to.

Advantage will be taken from the fact that ICT operators (e.g. telecom operators) have experience in securing information networks and this competence can be applied to new types of networks such as smart grids linking communication, energy and transport networks.

Expected impact:

Resilient and robust communication networks offering a reduced attack surface to the supported critical infrastructures. Reduced criticality of ICT components installed in critical infrastructures. Increased preparedness, reduced response time and coordinated response in case of a cyber-incident affecting communication and information networks. Reduce the possibilities to misuse ICT as a vehicle to commit cybercrime or cyber-terrorism.

Form of funding:

CP, Funding level: 70%

Specific call year:

This topic is part of the call for 2014

CONDITIONS FOR THIS CALL

Publication date: TBC by CNECT
Deadline: TBC by CNECT

Indicative budget: [Budgetary indications are not yet possible, due to the lack of agreement in the trilogues on the overall budget of Challenge 7]

Option 1: Indicative budget : EUR XXX million from the *[Insert year e.g. 2014 or 2015, in some cases both years could be mentioned]* budget

	2014 EUR million	*2015* *EUR million*	
Topics: 1, 2, 6	TBC	-------------------	*All single stage*
Topics: 3, 4, 5	-------------------	TBC	*All single stage*

Eligibility conditions:

The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Topics 1, 2, 3, 4, 5, 6,	The standard eligibility conditions apply. Please read carefully the provisions [*Link to the annex on standard eligibility conditions*] under Annex X before the preparation of your application.

Evaluation criteria:

The standard evaluation criteria apply. Please read carefully the provisions [*Link to the annex on standard evaluation criteria*] under Annex X before the preparation of your application.

Evaluation procedure: [*Link to the annex on standard evaluation procedure*]

- Proposal page limits and layout: 120 pages [TBC]
- Indicative timetable for evaluation and grant agreement[16]: *[as appropriate]*
  - *specify planned date to inform applicants of outcome of evaluation, and.*
  - *indicative date of signature of grant agreements or notification of grant decision*

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements
Topics: 1, 2, 6	TBC by CNECT	TBC by CNECT
Topics: 3, 4, 5	TBC by CNECT	TBC by CNECT

[16] Should the call publication postponed, the dates in this table should be adjusted accordingly.

Consortia agreements: *[as appropriate]*

[Standard sentence on climate change and/or sustainable development *[to be added as necessary]*

Other actions

Contents

Description for the other action topics on Galileo Public Regulated Services (PRS)

Financing the development of the security module for the **Galileo Public Regulated Service (PRS) will be addressed.** It should be noted that this development is about cryptology, secured design, etc. and is related to dual-use technology development; hence this corresponds largely to classified development. The proposed activities to be funded from the Horizon 2020 Security theme are only a part of the overall development, and that complementary tasks are expected to be carried out in the Space theme of Horizon 2020, as well as by some Member States.

Two specific public procurement actions are to be funded from the Security budget with 15 million for the first action and 5 for the second action. The procurement will be opened early in 2014, and the contracts are expected to be awarded by mid-2014, and will run for 30 months.

1 - PRS topic 1: Use of Galileo PRS in Professional Mobile Networks receiver, provision of an Early Service

The aim of the Galileo programme is to establish the first global satellite navigation and positioning infrastructure specifically designed for civilian purposes. The system established under the Galileo programme is completely independent of other existing or potential systems. The services offered through Galileo contribute, in particular, to the development of trans-European networks in the areas of critical infrastructure such as transport, telecommunications and energy infrastructures. The Public Regulated Service (PRS) is one specific objectives of the Galileo programme. This European GNSS service is restricted to government-authorised users, for sensitive applications which require a high level of service continuity.

From 2014 onwards, the exploitation phase of Galileo is set to begin with the deployment of Early Services. One of the biggest potential user communities for secure positioning, navigation and tracking is the one using Professional Mobile Radio (PMR) for Public Safety and Security (PSS). Indeed, missions of PSS are increasingly dependent on GNSS. At the same time, threats loom over GNSS and the critical applications using it.

The Public Regulated Service uses strong encrypted signals. However, the benefit of additional security comes with additional security constraints that may hamper critical applications from using the PRS. Previous studies have shown that those constraints can be made transparent to users by providing appropriate access control service based on use of an access control server and interconnectivity between the server and the terminals.

Further to those studies and demonstration activities, a full scale service shall be developed, deployed, accredited, and made available to Early Service demonstrations. A prototype of a receiver shall be developed. The objective is to use the all demonstrator it in 2016.

The research shall focus on the following points:

- Critical review of previous studies and demonstrations done by the Commission and the European GNSS Agency (GSA);
- Develop and deploy a demonstrator at full scale server;
- Develop a PMR receiver combined with PRS (following PRS4PMR demonstrator);
- Security certification and accreditation; and
- Provide logistic support to the operation of the service and its use for early services.

Expected impact:

Action under this topic shall provide significant improvement in the use of the Galileo PRS service by public safety and security user communities, in particular in critical infrastructure. The respect of the high level of security of PRS has to be demonstrated. By making this service available via networks, the cost to integrate PRS in PMR terminals will be minimized. This assumption has to be validated and demonstrated.

Type of action:

- Public procurement
- One single contract
- Pre-defined beneficiary: The European GNSS Agency (GSA)

Timeframe: XX quarter of 2014 (depending on the launch of the calls)

Indicative budget: EUR 15 million from the 2014 budget

2 - PRS Topic 2: Remote PRS processing server

This task is devoted to the setup of a server able to process PRS samples and to provide position velocity and time (PVT) as an output to the users. The idea behind this project is the concept of a “PRS Access Server”: a service provision based on a client-server architecture in which the client takes a snapshot of the Signal in Space (SIS) and provides it to the server that computes the PVT solution before sending it back to the client.

Given the challenges associated with development of fully-fledged security modules, the PRS Access Server may be the easiest way to deploy an early PRS service for some civilian users.

Starting from the activities already carried out by the GSA in this domain, this project should focus on:

- Consolidation of technical specifications;
- Definition of the system functional and physical architecture;
- Detailed design of the system;
- Detailed definition of internal and external interfaces;
- Development, assembly and integration of the different elements;
- Qualification testing and associated verification activities; and
- Acceptance testing.

Expected impact:

Action under this topic shall provide significant improvement in the use of the Galileo PRS service by public safety and security user communities.

Type of action:

- Public procurement
- One single contract
- Pre-defined beneficiary: The European GNSS Agency (GSA)

Timeframe: XXX quarter of 2014 (depending on the launch of the calls)

Indicative budget: EUR 5 million from the 2014 budget

3 - Supporting the implementation of the Security Industrial Policy and Action Plan through the European Reference Network for Critical Infrastructure Protection (ERNCIP)

With the publication of the Security Industrial Policy and Action Plan - COM(2012) 417 -, the European Commission has underlined the need and its ambition to foster the global competitiveness of the EU security industry, e.g. by promoting EU-wide standards of security technologies, tests and evaluations of security equipment, and respective certifications. ERNCIP, set up in the context of the European Programme for Critical Infrastructure Protection (EPCIP), is a direct response to the lack of harmonised EU-wide testing or certification for products and services (in the area of critical infrastructure protection), which is a barrier to future development and market acceptance of security solutions. This action should focus on linking the relevant work of ERNCIP with the implementation of the Security Industrial Policy and Action Plan, by supporting the uptake and promotion of identified activities. Relevant legislation on European and Member State level need to be taken into account appropriately, including potential ethical, societal and privacy issues of the proposed activities.

Legal entity: Joint Research Centre –Institute for the Protection and Security of the Citizen (IPSC) - Ispra (Italy)

Evaluation criteria: The Coordination and Support Action will be evaluated based on the evaluation criteria set out in Article XX of the Horizon 2020 rules of participation *[Link to the annex]*.

Rate of co-financing: The maximum possible rate of co-financing is set out in Article XX of the Horizon 2020 rules of participation *[Link to the annex]*.

Type of action: Grant to identified beneficiary - Coordination and Support Action

Indicative budget: EUR 0.5 million from the 2014 and the 2015 budget

4 – Evaluations of the proposals for the 2014 and 2015 calls "Fight against crime and terrorism"; "Disaster Resilient Societies" and "Border Security"

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

Type of action: Coordination and Support Action – Expert contracts

Indicative budget: Up to EUR 2.0 million from the 2014 and the 2015 budget

5 – Evaluations of the proposals for the 2014 and 2015 calls "Cybersecurity and Privacy"

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

Type of action: Coordination and Support Action – Expert contracts

Indicative budget: Up to EUR XX.XX million from the 2014 and the 2015 budget

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

a) Organisation of an annual Security Research event.

b) Support to workshops, expert groups, communications activities or studies

Workshops are planned to be organised on various topics to involve end-users, to support an expert group on societal issues, to prepare information and communication material etc.

Type of action: Public procurement. Several different contracts will be used including existing framework contracts.

Timeframe: Spread across from the first quarter of 2014 to the last quarter of 2015

Indicative budget: Up to EUR 1.9 million from the 2014 and from the 2015 budget

7 - Ex post evaluation of the FP7 Security Theme

The FP7 legal basis foresees the execution of an ex post evaluation: DECISION No 1982/2006/EC Article *"7 3. Monitoring, evaluation and review - Two years following the completion of this Framework Programme, the Commission shall carry out an external evaluation by independent experts of its rationale, implementation and achievements."*

On this basis, the evaluation should address notably the following questions:

How far has FP7 achieved its general objectives, including those of the specific programmes?

Does FP7 play an adequate role in positioning Europe on the global map of science and technology?

How can the impact and added value of collaborative research that cuts across scientific disciplines, industrial sectors and policy fields be further enhanced with a view to better address large societal challenges?

To what extent have simplification measures been effective?

What progress has been made under FP7 concerning the major issues which were highlighted in the FP6 evaluation report as needing further analysis, notably the participation, role and achievements of industry (including SMEs) in the Framework Programme?

Type of action: Coordination and Support Action – Expert contracts

Indicative budget: 500.000 from the the 2015 budget

Outlook on the 2016 calls

Two principles have always been at the core of the European efforts in security research: - ensuring the continuity of the past and on-going projects and - following a flexible and pro-active approach to effectively address the new security challenges faced by the EU.

One of the priorities of the 2016 Secure Societies calls will therefore be to build upon the results of existing projects.

Among topics of the 2016 calls will thus be two large scale demonstration projects entitled: “Factors affecting (in-) security” and “Strengthening capacity-building for health and security protection in case of large-scale pandemics”. Both topics will be based on the results of the two demonstration phase 1 projects included respectively in the 2014 “Fight against crime and terrorism” and “Disaster Resilient Societies” calls. A Pre Commercial Procurement topic for 2016 will build upon the results of the “Crisis management topic 5: Situation awareness of Civil Protection decision-making solutions – preparing the ground for a PCP”.

Horizon 2020 will also continue to support the implementation of the EU security policy initiatives, such as the EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673), the EU CBRN Action Plan (COM(2009) 273), the EU Action Plan on the security of explosives (COM(2007) 651), the Communication “Towards a stronger European disaster response: the role of civil protection and humanitarian assistance” (COM (2010) 600) and the "Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace" (JOIN (2013) 1).

Further topics for the 2016 calls will be developed through discussions with Member States, relevant stakeholders, NIS platform, as well as through dedicated Workshops and Conferences.