HORIZON 2020

WORK PROGRAMME 2014 – 2015

14. Secure societies – Protecting freedom and security of Europe and its citizens

Important Notice on the First Horizon 2020 Work Programme

This Work Programme covers 2014 and 2015. Due to the launching phase of Horizon 2020, parts of the Work Programme that relate to 2015 (topics, dates, budget) are provided at this stage on an indicative basis only. Such Work Programme parts will be decided during 2014.

(European Commission Decision C (2013)8631 of 10 December 2013)

Table of contents

Introduction

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

The primary aim of this Work Programme is thus 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 1); to fight crime and terrorism ranging from new forensic tools to protection against explosives (call 2); to improve border security, ranging from improved maritime border protection to supply chain security and to support the Unions external security policies including through conflict prevention and peace building (call 3); and to provide enhanced cybersecurity (call 4), ranging from secure information sharing to new assurance models. Proposers are encouraged to use, where appropriate, the services provided by European space-based systems (e.g. EGNOS, Galileo or Copernicus).

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 responding to well identified needs by the end-users, be it market operators, security agencies or the citizens. Therefore the latter

[1] COM(2012)417 final
[2] COM(2010) 673 final
[3] JOIN(2013)1 final

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 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 entities(typically national or European agencies or authorities).

A novelty in Horizon 2020 is the Open Research Data Pilot which aims to improve and maximise access to and re-use of research data generated by projects. While certain Work Programme parts and areas have been explicitly identified as participating in the Pilot on Open Research Data, individual projects funded under the other Horizon 2020 parts and areas can choose to participate in the Pilot on a voluntary basis. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research. Further guidance on the Open Research Data Pilot is made available on the Participant Portal.

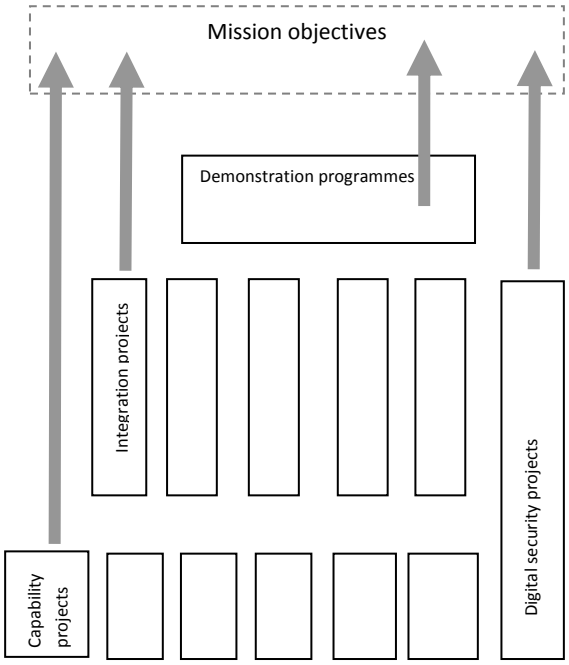

Figure 1: Research instruments to meet the Secure Societies' objectives

Call - Disaster-resilience: safeguarding and securing society, including adapting to climate change[45]

H2020-DRS-2014/2015

Securing the society against disasters is one of the central elements of the functioning of any society. There is barely any societal sector which is not to some extent concerned by disasters and related resilience and security issues. The objective of this call is to reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including extreme weather events, crime and terrorism threats.

This area will therefore focus on developing technologies and running large-scale demonstration with a view to:

This call is divided in five parts:

1. Crisis Management and Civil protection with a view to strengthening prevention and preparedness against natural and man-made disasters by underpinning an all-hazard approach to risk assessment across the EU;
2. Disaster Resilience and Climate Change with a view to developing solutions, for climate change adaptation in areas potentially affected by more extreme weather events and natural disasters, such as for port cities, critical infrastructures, tourism;
3. Critical Infrastructure Protection with a view to building up community resilience and resilience of critical infrastructure, including against cyber-crime and cyber-terrorism.
4. Communication Interoperability facilitating disaster management, notably through communication technologies for crisis response actors and the linking of situational awareness centres;
5. Ethical/Societal Dimension.

Proposals are invited against the following topics:

[4] Any activity, resulting from this call that manages classified information, is excluded from the delegation to REA and will be implemented by the Commission services.

[5] Some activities, resulting from this call, may involve using classified background (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification in accordance with the relevant Guide for Classification. For those activities in particular, *but not exclusively:* DRS 2, 3, 12, 14, 17, 21, proposers are invited to anticipate to the maximum extent possible the requirements for handling security sensitive information. The final decision on the classification of projects is subject to a Security Scrutiny Process. The Time To Grant will start from the completion of the Security Scrutiny Process.

I. Crisis management

DRS-1-2015: Crisis management topic 1: Potential of current and new 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 and related landslides, storm surges, heatwaves, fires, including vegetation fires) have increased in frequency or magnitude, and in the meantime populations and assets at risk have also increased, leading to enhanced disaster risks. In order to better forecastand manage the immediate consequences of weather- and climate-related disasters, in particular regarding emergency responses, improved measures and technologies are needed.

Scope: Proposals should focus on the potential of current and new measures (including local measures) and technologies to enhance the response capacity to extreme weather and climate events affecting the security of people and assets. Proposals should focus on emergency management operations and cover the whole crisis management, linking awareness and early warning to effective responses within society and coordination with first responders, including the use of adapted cyber technologies to gain time and improve coordination in emergency situations. Proposals 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.

The Commission considers that proposals 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.

In line with the EU's strategy for international cooperation in research and innovation[6] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

Expected impact:

- more effective and faster emergency responces to extreme weather and climate events; Faster analysis of risks and anticipation;
- publicly available online now- and fore-casting systems for disasters triggered by (extreme) weather conditions**;**
- improved coordination of emergency reactions in the field;
- improved capacity to provide adequate emergency responses to extreme weather and climate events;
- shorter reaction time and higher efficiency of reactions;
- enhancement of citizen's protection and saving lives.

The action is expected to proactively target the needs and requirements of users, such as national law enforcement agencies, climate and weather services, civil protection units and public and private operators of critical infrastructures and networks.

[6] COM(2012)497

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-2-2014 Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination and/or exposure

Specific challenge: A fast detection of exposure or contamination with CBRN substances (including toxins) using traceable tools and rapid identification of critically exposed individuals 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 CBRN incident is therefore needed to differentiate between contaminated and/or exposed persons and those individuals 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 have been exposed/contaminated or not (by a CBRN agent) as well as the level of contamination / exposure (including making use of point of care diagnostic tests), develop and 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. A special attention should be given to gender, ethical, religious and privacy aspects, for instance for pregnant women, disabled individuals, etc. The ethical implications and social acceptance of the proposed solution needs to be studied, contributing to an improved cooperation between science and society. Dual-use aspects will be considered with possible synergies being established with the European Defence Agency. Existing networks of end users from all affected fields (e.g. defence/security experts, firemen, rescuers) need to be actively involved in both technologies and procedures.

The Commission considers that proposals 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:

- faster and more efficient treatments, detection and monitoring technologies of exposure to or contamination with CBRN substances (including toxins) in the case of accidents or terrorist attacks;
- new integrated, interoperable and centralised system to improve the triage and monitoring of victims, including the reduction of risks of cross-contamination between non-contaminated and contaminated victims.
- improved CBRN (including toxins) detection and monitoring capabilities;
- improved crisis management in case of a mass contamination/exposure through integration of information via a centralised system, involving all relevant stakeholders.
- improved cooperation between science and society through ethical screening of the developed solutions;
- higher cost-efficiency through dual-use applications;
- contribution to ongoing standardisation work.

The action is expected to proactively target the needs and requirements of users, such as national law enforcement agencies, first responders and civil protection units in the CBRN area.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-3-2015: Crisis management topic 3: Demonstration activity on large scale disasters and crisis management and resilience of EU external assets against major identified threats or causes of crisis[7]

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 management. Various measures can be employed to assess management and resilience of major natural and man-made disasters. However, more research is needed in this field of study on factors that contribute to effective management of major disasters and crisis, including risk analysis and cost modelling. In particular, demonstration is needed to further improve on-field management of international and humanitarian crises operations, civil protection assistance, including deployment (before and after a crisis) of EU teams, materials and services (humanitarian logistics), possibly repatriation of EU citizens.

Scope: The demo should aim at demonstrating the EU deployable disaster and crisis management capabilities to be applied in real situations outside the EU. The proposals should investigate the consequences of poor and/or late situational awareness reducing the ability to comprehend the scale of a crisis, taking into account the identification of risk areas and vulnerable groups, especially for people with mobility, hearing and sight problems. Proposals should explore the cost-saving effect of comprehensive risk and threat prevention systems as well as the management cycle from the detection of a crisis event, the planning of actions and the prioritization of efforts through the mobilization of responders to the delivery of information to the responders on siteIt should combine dynamic data (from sensors, aerial networks etc.) with static information (maps, infrastructure, assessment templates) keeping in mind the security of the information exchanged. 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 expected to link policy, research and end-users in order to make it useful at the end, thus directly contributing to improving cooperation between science and society. It should bridge the current gaps and allow testing and validating research solutions that a later stage could be applied directly for disaster management.

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 disasters and 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

[7] 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

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 management.

Cost-efficiency should be introduced in all aspects of the disaster management activities. As such the demo should include it as a key factor (best use of available resources). In particular, the costs of coordination activities and logistics 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.

The demo should build on existing tools and results of completed and ongoing Seventh Framework Programme and national 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.

The demo should give importance to integrating adaptation to climate change and disaster risk management.

In line with the EU's strategy for international cooperation in research and innovation[8] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

The Commission considers that proposals requesting a contribution from the EU of between €10m and €20m EUR would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

- increasing our capacity to anticipate, prepare and respond to disasters occurring outside the EU - including those potentially affecting EU external assets - through better risk assessments, monitoring and planning, including an improved use of existing assets and logistics;
- enhanced capability to deploy disaster and crisis management assets in real situations outside the EU;
- faster assessement and feedback of data to coordination centres and communication;
- improved prevention, preparedness, response in line with the EU and the UN approach to Disaster Risk Reduction;

[8] COM(2012)497

- enabling a better risk assessment and improved decision-making;
- improved communication and coordination of response actions and sharing of information with the public;
- boosting the competitiveness and visibility of EU disaster and crisis management services.

will also contribute to

- support EU policy priorities in the area of disaster and crisis management , where serious major disasters orcrisis require immediate action and that may affect the lives, infrastructures, the environment and EU external assets.
- 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;
- take into account the recently adopted legislation on the Civil Protection Mechanism.

The action is expected to proactively target the needs and requirements of users, such as national and local law enforcement agencies, civil protection units and first responders.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-4- 2014: 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 viable innovative concepts. Approaches should integrate relevant research as well as aspects related to risk assessment, communication, education and governance, thus contributing to improve cooperation between science and society. Concepts should be developed with a view to cross-border approaches. The proposal should aim at identifying gaps and research and priorities to be addressed in a second phase focusing on demonstration.

In line with the EU's strategy for international cooperation in research and innovation[9] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

[9] COM(2012)497

Expected impact: The central aim of this topic is to prepare a future large scale demonstration project on large scale pandemics.

The following impacts are expected:
- 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;
- identification of innovative concepts that would allow to better integrate existing tools and systems for a strengthened capacity-building for health and security protection in case of large-scale pandemics;
- analysis of feasability of a future demonstration project.

The action is expected to proactively target the needs and requirements of users, such as health and security agencies, civil protection units and first responders.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-5-2014: Crisis management topic 5: Situation awareness of Civil Protection decision-making solutions – preparing the ground for a Pre-commercial Procurement (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 and Associated Countries at national, regional and local level in risk prevention in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union; b) promote swift effective cooperative action within the EU between national civil protection services; c) promote consistency in international civil protection actions. A comprehensive European approach on security issues based on the capitalization of knowledge existing at EU and national level will considerably help the development and implementation of civil protection decision-making solutions.

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

Proposals 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)), sensors and tools (e.g. situation awareness) in order to make them more cost effective and interoperable.

Expected impact:

- create a network of potential procurers, including through the exchange of experiences between (public) stakeholders on civil protection and;

- 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;
- create a roadmap for a future PCP topic to be included for an upcoming Horizon 2020 Secure Societies research call;
- outline perspectives for large-scale testing and simulation of civil protection solution with the view to improve decision-making solutions at national and European levels;
- improved cooperation between science and society, in particular encouraging citizens to engage in science and improving the effectiveness of interactions between scientists, civil protection stakeholders, general media and the public.

Type of action Coordination and Support Actions

Additional condition: A central condition for a successful PCP project is the participation of end–users from relevant public authorities. A project in preparation of a PCP should therefore follow the same principles. This topic will therefore require the participation of relevant public authorities from at least 3 Member States and Associated Countries..

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-6-2015: 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, 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[10], how a cross-fertilisation of work between the proposal and these relevant activities will be

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

achieved and how the proposal consortium intends to involve itself in relevant CEN and/or ISO TC's.

Expected impact:

- better assessment of feasibility and impact of standards in the area of disaster resilience;
- establishment of a standardisation roadmap;
- improved coordination of activities and cross-fertilisation among different sectors;
- improved disaster resilience of EU population, crisis management / civil protection and/or CBRNE systems, tools and services

The action is expected to proactively target the needs and requirements of users, such as standardization bodies, security agents in the CBRNE area and civil protection units.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-7-2014: Crisis management topic 7: 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 and Associated Countries. This concerns both man-made threats (accidents, terrorism) and natural hazards such as e.g. floods, storms, earthquakes, volcanoes and tsunamis.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 population, the media, rescuers (staff, volunteers and ad-hoc volunteers). . 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 link and share EU-wide risk assessment and mapping approaches[11] with relevant resilience management approaches, to ensure that risk assessment

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

is followed by the development of resilience concepts in the various security sectors, based on the results of the risk assessments.

Scope: Proposals 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, or other appropriate 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) [12] programme and its successor in the Internal Security Fund, and that it is linked to the *"European Programme for Critical Infrastructure Protection"* (EPCIP) programme[13] and its new revised approach. Findings from relevant Seventh Framework Programme projects need to be taken into account, and integrated into the research where possible. Furthermore, a close collaboration with the major EU demonstration 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 proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

- the development of European Resilience Management Guideline and demonstration through pilot implementation;
- more efficient uptake of risk assessments through Member States and Associated Countries and Critical Infrastructure Providers; and
- more effective and coherent crises and disaster resilience management, including improved trainings for rescuers and population engagement.

The action is expected to proactively target the needs and requirements of users, such as civil protection units, first responders and critical infrastructure providers.

Type of action: Research & Innovation Actions

[12] 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)

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

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-8-2014: Crisis management topic 8: Trans-national co-operation among National Contact Points (NCPs) for Security

Specific challenge: For editorial reasons, this topic is presented under the Disaster Resilient Societies call but the topic relates to the whole secure societies challenge.

Facilitate trans-national co-operation between NCPs within this Societal challenge with a view to identifying and sharing good practices and raising the general standard of support to programme applicants, taking into account the diversity of actors that make up the constituency of this Societal challenge.

Scope: Support will be given to a consortium of formally nominated NCPs in the area of security research. The activities will be tailored according to the nature of the area, and the priorities of the NCPs concerned. Various mechanisms may be included, such as benchmarking, joint workshops, enhanced cross-border brokerage events, specific training linked to this societal challenge as well as to gender dimension of Research and Innovation, and twinning schemes. Special attention will be given to enhance the competence of NCPs, including helping less experienced NCPs rapidly acquire the know-how accumulated in other countries.

The focus throughout should be on issues specific to the secure societies societal challenge and should not duplicate actions foreseen in the NCP network for quality standards and horizontal issues under "Science with and for Society".

Proposals can only include NCPs from EU Member States, Associated Countries and Third Countries that have demonstrated in the past a particular interest in the themes covered by this societal challenge, who have been officially appointed by the relevant national authorities. The consortium should have a good representation of experienced and less experienced NCPs.

Submission of a single proposal is encouraged. NCPs from EU Member States or Associated Countries choosing not to participate as a member of the consortium should be identified and the reason explained in the proposal. These NCPs are nevertheless invited and encouraged to participate in the project activities (e.g. workshops), and the costs incurred by the consortium for such participation (e.g. travel costs paid by the consortium) may be included in the estimated budget and be eligible for funding by the Commission.

Expected impact:

- An improved and professionalised NCP service across Europe, thereby helping simplify access to Horizon 2020 calls, lowering the entry barriers for newcomers, and raising the average quality of proposals submitted.
- A more consistent level of NCP support services across Europe.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

II. Disaster Resilience & Climate Change

DRS-9-2014/2015: Disaster Resilience & Climate Change topic 1: Science and innovation for adaptation to climate change: from assessing costs, risks and opportunities to demonstration of options and practices

Specific challenge: As the EU, the Member States, Associated Countries and the EU Overseas Countries and Territories (OCTs) progress towards the development of appropriate responses for adapting to climate change, there is a pressing need for developing a coherent research and innovation agenda, to provide:

- The coordination and the clustering of research and innovation activities on climate change impacts, vulnerabilities and adaptation in different sectors, also in relation to long-term risk reduction from extreme weather events;
- A more standardised basis (including transferable, widely applicable tools and methods) for assessing potential climate change impacts, vulnerabilities, costs, benefits, risks and opportunities;
- A strengthened knowledge base, through a more coherent approach to the identification and assessment of the performance and impacts of different adaptation measures, with a view to prioritise relevant interventions;
- Support for the development of innovative adaptation and long term risk reduction options, fine-tuned to specific natural and socio-economic conditions across Europe, with the aim to protect and reduce the vulnerability of sensitive resources, economic sectors, green and technical infrastructure, and society from climate-change related threats.

Scope: Proposals must address one of the following (a,b,c):

a) **Coordination and support actions [2014][14]**

Proposals should aim to:

- Develop a platform to organise consultations and facilitate dialogue among different stakeholder groups at the EU and Associated countries level and at different geographical scales, throughout the duration of Horizon 2020, paying due attention to, and establishing linkages with international developments in the field; as well as
- Support clustering and close cooperation among international, EU and nationally funded initiatives in the field of climate change adaptation, and disaster risk reduction, promote foresight and large-scale dissemination activities, and foster the science-policy interface across the EU.

The action is expected to proactively target coordination needs and requirements of end-users, such as the Commission services dealing with climate change adaptation, EU, national, regional and local authorities that manage a prospective research agenda in this field, as well as key actors that participate in the development and implementation of adaptation strategies and in the mainstreaming of adaptation requirements into sectoral plans.

[14] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies and supporting various groups of stakeholders is excluded from the delegation to EASME and will be implemented by the Commission services.

The Commission considers that proposals requesting a contribution from the EU between the range of 2 to 3 million euro would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

b) **Research and innovation actions [2014]**

Proposals should aim to:

- Develop standardised methods to assess climate change impacts, vulnerabilities, and risks, and to identify and assess the performance of adaptation measures (technological and non-technological options). Methods should focus on long-term climate change and extreme events for European sectors of particular socio-economic and environmental significance, paying due consideration to uncertainty, and encompass indirect, cross-sectoral effects and cascade impacts, where relevant.
- Provide state-of-the-art decision support tools tailored to facilitate decision-making by different end-users (e.g. individuals, businesses, other private sector firms, local authorities and planners, governments), while developing adaptation plans and measures.

The ambition of the challenge suggests that proposals with a requested EC contribution in the range of €6 million to €8 million (or more) may be appropriate. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

c) **Innovation actions [2015]**

Proposals should aim to:

- Support, test and disseminate technological and non-technological options, including eco-system based approaches, to address climate-related risks and climate-proof critical infrastructure assets and systems;
- Develop frameworks for monitoring the performance and effectiveness of developed approaches, and for ensuring their optimum performance, addressing also post-implementation requirements, as well as operational and organisational/governance needs for successful replication and follow-up;
- Provide innovative solutions for major implementation projects at local, regional or national levels, while strengthening complementarity with other EU funding mechanisms, and particularly with the European Structural and Investment Funds.

The Commission considers that proposals requesting a contribution from the EU between the range of 6 to 8 million euro would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

<u>Expected impact:</u>

a) Better coordination, dissemination and communication of research and innovation activities on disaster risk management, climate change adaptation and synergies among EU-funded (e.g. ClimateAdapt, Climate KIC, FP projects), Member State-funded (e.g. JPIs, national programmes) and international activities in the field (e.g. UNEP/PROVIA).

b) Improved and concise information for decision making (at both public and private sectors) on climate change impacts, disaster risks and relevant options to address them. Enhanced implementation in the medium-term of the EU Adaptation Strategy and national and local efforts towards climate-proofing of key European economic sectors and services, as well as of the EU Disaster Prevention Framework.

c) Rapid large-scale deployment and market uptake of innovative technological and non-technological climate change adaptation solutions with high replicability. Contribution to the development of technological and performance standards for adaptation options.

Type of action*:*

a) Coordination and support actions

b) Research and innovation actions

c) Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-10-2015: Disaster Resilience & Climate Change topic 2: Natural Hazards: Towards risk reduction science and innovation plans at national and European level[15]

Specific challenge: Previous and recent catastrophic events have demonstrated that society has become more and more vulnerable and exposed to risk also in an uneven distribution way at global level. A more coherent approach to threat and related risks needs to be developed within a strong risk reduction innovative frame and perspective to organise and structure, with all the relevant actors, a contribution to a new strategy for future research activities in natural hazards going beyond the traditional risk concepts and including resilience;

Scope: Proposals should aim to:

- develop an efficient networking and forum promoting effective mechanisms and interactions with the key players (e.g. scientists, authorities, users, civil protection, UNISDR platforms...) in order to contribute to a new strategic vision on natural hazards risk reduction;
- identify the necessary key actions to be promoted (short to long term perspective), building on new concepts and innovations, in order to improve interdisciplinary scientific knowledge and apply or adapt current tools and methods to a new and effective risk reduction strategy at national/European level;
- 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.

The Commission considers that proposals requesting a contribution from the EU between the range of 2 to 3 million euro would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

[15] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies and supporting various groups of stakeholders is excluded from the delegation to EASME and will be implemented by the Commission services.

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 research and innovation agenda in this field. Enhanced implementation of the EU disaster prevention framework including preparatory work supporting guidelines on risk management capability, as called for in the forthcoming Civil Protection legislation (article 5e).

The action is expected to proactively target the "coordination" needs and requirments of users, such as the UNISDR European national Platforms; the Commission services dealing with prevention, risks and disasters issues, the national authorities managing a prospective research agenda related to natural hazards; the key actors implementing disaster risk reduction measures related to natural hazards.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-11-2015: Disaster Resilience & Climate Change topic 3: Mitigating the impacts of climate change and natural hazards on cultural heritage sites, structures and artefacts

Specific challenge: Europe's cultural heritage is being lost at an alarming rate, not only due to natural decay and human impacts but frequently also as a result of environmental changes, climatic conditions or natural hazards. This non-renewable resource, in all its diverse physical forms needs safeguarding for future generations. Cultural heritage, an important component of individual and collective identity, also fuels Tourism in Europe, a significant economic sector on which many communities depend. However, the increased frequency and intensity of extreme weather events together with risks associated to natural hazards present an added challenge for the sustainable management and conservation of cultural heritage in Europe, calling for improved adaptation and mitigation strategies in this vulnerable sector.

Scope: The proposal should aim to develop eco-innovative solutions to help mitigate the effects of climate change and natural hazards on cultural heritage sites, structures and artefacts taking into account the values they hold for people and respecting their historic and cultural integrity. Effective adaptation strategies, systems and technologies are needed for better risk management of vulnerable heritage materials and for mitigating damage to cultural heritage assets. Proposals may include case studies and address any research gaps or barriers needed to respond to this challenge, including aspects relating to innovative environmental assessment methodologies, integrated monitoring technologies and systems, improved non-invasive and non-destructive methods of surveying and diagnosis including wide area surveillance, cost-effective conservation and restoration techniques, risk management, disaster prevention and quick damage assessment when catastrophes occur.

The Commission considers that proposals requesting a contribution from the EU between the range of 6 to 8 million euro 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 sustainable and effective safeguarding and management of European cultural heritage through more reliable predictive and cost effective maintenance, improved

risk management, diagnosis and treatment and a better understanding of the historical and technological contexts of heritage materials and objects. More effective advice and input to restoration and adaptation policies of government organisations thereby promoting improved practices for the guardians of cultural heritage assets. Reduced fragmentation in this sector through increased collaboration and cooperation and a fostering of an interdisciplinary approach.

The action is expected to proactively target the needs and requirements of users,such as decision makers at local, regional, national and international level responsible for disaster mitigation and safeguarding of cultural heritage assets.

Type of action: Research & Innovation Actions

III. Critical Infrastructure Protection

DRS-12-2015: 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. The same is applicable to all utility supply networks (e.g. water or gas system supply). The systems and meters of the charge points for electrical cars should be also a concern, specially considering the increasing market for this type of vehicles

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 resilience 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 be developed, which shall also take into account the urban areas implications (i.e. the general public subscribing to this service). The proposal shall provide concrete solutions for securing public and private critical networked infrastructures and services against the above mentioned threats.

A key characteristic of the Smart Grid is that it consists of millions of devices, spread across organizations and households in a vast geographical area. In case of a Public Key Infrastructure (PKI) usage, a utility company would face an extreme credential management overhead and logistic costs of maintenance. This means that new security management schemes must be designed and evaluated for the Smart Grid to meet its high scalability requirements.

Security solutions must take into account that an adversary has a physical access to smart meters. These devices' cost, power, memory, and computational limitations restrict the ability to deploy standard trusted platform modules on them. Due to the fact that smart meters will be deployed for many years, novel cryptographic solutions should be tested that include message encryption, authentication and integrity, along with the highest possible levels of efficiency in time-critical and high volume data

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.

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.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately appropriately (similar to the FP7 Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

- higher protection levels of energy distribution grid infrastructures:
- more effective and systematic approach to resilience enhancements of smart grid critical infrastructures when new components are added:
- improved applicability through small scale proof of concept of system to demonstrate the "resilience" of the proposed "system":
- increased understanding of technology providers on modern operational requirements thus increasing their competitiveness.

Type of action: Research & Innovation Actions

The action is expected to proactively target the needs and requirements of public bodies and industry.
The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 4; please see part G of the General Annexes.

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-13-2015: Critical Infrastructure Protection topic 2: Demonstration activity on tools for adapting building and infrastructure standards and design methodologies in vulnerable locations in case of natural or man-originated 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 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. As a complement to current research in this area, and based on the knowledge of risks (natural or man-originated) in vulnerable areas in Europe, building standards should be developed and tested, applying a number of technological means and design procedures.

Scope: 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.

The 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 topic will complement Seventh Framework Programme research focusing on impacts of extreme weather on critical infrastructure.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately (similar to the FP7 Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact: More effective building standards and design methodologies for infrastructures and households located in vulnerable areas. Enhanced security of citizens and assets in such areas. Reduced socio-economic impact of natural catastrophes.

The action is expected to proactively target the needs and requirements of public bodies.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL)7; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-14-2015: 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 natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks).

Scope: A holistic approach to the resilience of critical infrastructure should be followed, addressing a broad variety of issues including: human factors (i.e. radicalization), security, geo-politics, sociology, economy, etc. and increased vulnerability due to changing threats.

Critical Infrastructure resilience is the ability to reduce the impact of disruptive events and the recovery time. 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.

The proposal shall demonstrate that a set of common and thoroughly validated indicators, including economic indicators, 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 (energy grids, transportation, government, nuclear research infrastructures, water, etc.). The developed methodology shall be based on at least four types of critical infrastructure as test cases. Specific models and modeling approaches will be proposed and developed that facilitates the understanding and modeling of security risks and the related impact. Moreover, security metrics and indicators will be proposed that could be used in the developed models to quantify to the possible extent the considered risk and impact as well as give guidance to the possible mitigation techniques – approaches.

New methods and solutions of assessing resilience based upon comprehensive threat, criticality, and vulnerability assessments are of outmost importance. Proposals should follow a uniformed, comprehensive, and holistic approach at all levels (e.g. EU, country, local) including private organizations charged with protecting citizens, facilities, and infrastructure in order to anticipate current and emerging threats and security challenges.

Integrated concepts of resilience in interconnected infrastructures and cascading effects that have a devastating impact on the functioning of society should also be included.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately (similar to the FP7 Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact: Better risk assessment of different areas of critical infrastructures (energy grid, water supply, transport, communication, etc.) by taking into account interdependencies. More effective and comprehensive methodology using 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).

The action is expected to proactively target the needs and requirements of public bodies.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 4; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-15-2015: 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 (inter-)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.. Small-scale demonstration activities focusing on SMEs should be considered.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately (similar to the Seventh Framework Programme Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

- better preparedness to Seveso type site/area related accidents via improved protection measures (including people training and education);
- more effective assessment and decision-making related to the potential severity of a CBRNE accident, in particular regarding ways to decrease the cost of this kind of crisis and develop adequate protection measures in the light of established policy goals:
- better risk assessment to evaluate different sectors, regions or populations for comparing them in terms of relative vulnerability to help set priorities that can guide the allocation of protecting measures financing appropriately;
- enhanced understanding by policy-makers and other stakeholders on 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).

The action is expected to proactively target the needs and requirements of public bodies and industry.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL)7; please see part G of the General Annexes.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-16-2014: Critical Infrastructure Protection topic 6: Improving the aviation security chain

Specific challenge: Aviation Security is governed by EU legislation (such as Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection) and implemented at airports (checkpoint for passengers and staff, hold baggage and air 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[16], Flightpath 2050[17] and IATA check point of the future[18].

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. The development of the detection technology needs to be threat-based and take stock of the latest terrorist development in particular the threat materials and concealment methods of e.g. home-made explosives, chemical, biological, radiological and nuclear threats.

Scope: The proposal should therefore 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.

While proposal should aim to deliver solutions for higher levels of security and facilitation it should be developed and tested to assess their impact and viability. Realistic estimations and

[16] COPRA Aviation Security Research Roadmap: http://www.copra-project.eu/Results.html
[17] Flightpath 2050: Europe's vision for aviation: http://ec.europa.eu/transport/modes/air/doc/flightpath2050.pdf
[18] IATA Checkpoint of the Future: http://www.iata.org/whatwedo/security/pages/checkpoint-future.aspx

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 Seventh Framework Programme projects should be taken into account.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately(similar to the Seventh Framework Programme Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

In line with the EU's strategy for international cooperation in research and innovation[19] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

Expected impact: Higher level of threat and risk-based security and a reduced operational impact on passengers and industry. Faster, more accurate and reliable, less invasive, and overall more efficient to operate systems and processes than existing ones throughout their lifetime.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-17-2014/2015: Critical infrastructure protection topic 7: SME instrument topic: "Protection of urban soft targets and urban critical infrastructures"

Specific challenge: The aim is to engage small and medium enterprises in security research and development and in particular to facilitate and accelerate the transition of their developed products/services to the market place ,.

[19] COM(2012)497

The specific challenge of the actions and activities envisaged under this topic are related to protection of urban soft targets and urban critical infrastructures .

Specific consideration should be given to 'urban soft targets' , which are exposed to increasing security threats which can be defined as urban areas into which large numbers of citizens are freely admitted, for usual activities or special events or routinely reside or gather. Among others, these include parks, squares and markets, shopping malls, train and bus stations, passenger terminals, hotels and tourist resorts, cultural, historical, religious and educational centres and banks.

The critical infrastructures sectors listed in the European Programme for Critical Infrastructures Protection (EPCIP)[20], including, among others, energy installations and networks, communications and information technology, finance (banking, securities and investment), water (dams, storage, treatment and networks), supply chain and government (e.g. critical services, facilities, information networks, assets and key national sites and monuments) are not only relevant at a national scale but they can be considered critical infrastructures in an urban context as well.

The objective is to carry out a small-scale demonstration of innovative technologies and tools.

Taking into consideration the results of past and on-going EU and international research in this field, they can cover any aspect of the urban critical infrastructure protection, such as, for example: designing buildings and urban areas; protection of energy/transport/communication grids; critical infrastructure surveillance solutions; protecting supply chains; avoiding cyber-attacks and developing cyber resilience systems for critical infrastructures.

The scope of this topic is focused to cover, for example:

- high throughput screening of people and their bags including the ability to screen them in reasonably real-time as people approach entrances to buildings or enter public transportation system;
- high throughput screening for vehicles to identify threats that warrant further inspection (as opposed to random searching);
- potential CBRN-E threats and the way in which these threats could be carried-out against soft targets and critical infrastructures;
- mitigation of vehicle-borne improvised explosive devices, with a specific focus on vehicle-borne ones (e.g. in cases of parked vehicles, penetrative attacks, etc.).

The action is expected to proactively target the needs and requirements of users, such as national law enforcement agencies public and and private operators of critical infrastructures and networks.

Scope: The SME instrument consists of three separate phases and a coaching and mentoring service for beneficiaries. Participants can apply to phase 1 with a view to applying to phase 2 at a later date, or directly to phase 2.

[20] COM(2006) 786 final – Official Journal C 126 of 7.6.2007

In phase 1, a feasibility study shall be developed verifying the technological/practical as well as economic viability of an innovation idea/concept with considerable novelty to the industry sector in which it is presented (new products, processes, design, services and technologies or new market applications of existing technologies). The proposals could, for example, comprise risk assessment, market study, user involvement, Intellectual Property (IP) management, innovation strategy development, partner search, feasibility of concept and the like to establish a solid high-potential innovation project aligned to the enterprise strategy and with a European dimension. Bottlenecks in the ability to increase profitability of the enterprise through innovation shall be detected and analysed during phase 1 and addressed during phase 2 to increase the return in investment in innovation activities. The proposal should contain an initial business plan based on the proposed idea/concept.

The proposal should give the specifications of the elaborated business plan, which is to be the outcome of the project and the criteria for success.

Funding will be provided in the form of a lump sum of EUR 50.000. Projects should last around 6 months.

In phase 2, innovation projects will be supported that address the specific challenge of protecting urban soft targets and critical infrastructures and that demonstrate high potential in terms of company competitiveness and growth underpinned by a strategic business plan. Activities should focus on innovation activities such as demonstration, testing, prototyping, piloting, scaling-up, miniaturisation, design, market replication and the like aiming to bring an innovation idea (product, process, service etc) to industrial readiness and maturity for market introduction, but may also include some research. For technological innovation a Technology Readiness Levels (TRL) of 6 or above (or similar for non-technological innovations) are envisaged; please see part G of the General Annexes.

Proposals shall be based on an elaborated business plan either developed through phase 1 or another means. Particular attention must be paid to IP protection and ownership; applicants will have to present convincing measures to ensure the possibility of commercial exploitation ('freedom to operate').

Proposals shall contain a specification for the outcome of the project, including a first commercialisation plan, and criteria for success.

The Commission considers that proposals requesting a contribution from the EU of between EUR 0.5 and 2.5 million would allow phase 2 to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requestion other amounts. Projects should last between 12 and 24 months.

In addition, in phase 3, if any, SMEs can benefit from indirect support measures and services as well as access to the financial facilities supported under Access to Risk Finance of this work programme.

Successful beneficiaries will be offered coaching and mentoring support during phase 1 and phase 2. This service will be accessible via the Enterprise Europe Network and delivered by a dedicated coach through consultation and signposting to the beneficiaries. The coaches will be recruited from a central database managed by the Commission and have all fulfilled stringent criteria with regards to business experience and competencies. Throughout the three phases of the instrument, the Network will complement the coaching support by providing access to its innovation and internationalisation service offering. This could include, for example, depending on the need of the SME, support in identifying growth potential, developing a growth plan and maximising it through internationalisation; strengthening the

leadership and management skills of individuals in the senior management team and developing in-house coaching capacity; developing a marketing strategy or raising external finance.

Expected impact:

- Enhancing profitability and growth performance of SMEs by combining and transferring new and existing knowledge into innovative, disruptive and competitive solutions seizing European and global business opportunities.
- Market uptake and distribution of innovations tackling the specific challenge protecting urban soft targets in a sustainable way.
- Increase of private investment in innovation, notably leverage of private co-investor and/or follow-up investments.
- The expected impact should be clearly described in qualitative and quantitative terms (e.g. on turnover, employment, market seize, IP management, sales, return on investment and profit).

Type of action: SME instrument 70% funding

The conditions related to this topic are provided at the end of this call and in the General Annexes.

IV. Communication technologies and interoperability

DRS-18-2014: Communication technologies and interoperability topic 1: interoperable next generation of broadband radio communication system for public safety and security – Pre-commercial Procurement (PCP)[21] [22]

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, seamless, interoperable (also in degraded conditions) and cost efficient PPDR broadband communication systems, while preserving the investment done on the currently deployed systems.

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

1) Technology review and specifications definition

[21] For this topic specific rules related to Article 25.5 "Option 1*"* and Article 31.5 *"*Option 4*"* of the model grant agreement may apply

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

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, also when 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 specifically comprise of:

- Identifying and analyzing common communications requirements of PPDR; 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 research phase

This phase may include a very short research effort, also quite limited in scope, where the extensive research activities that occurred throughout the Seventh Framework Programme are fully taken into account.

3) 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.

4) 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 (fire brigades, medical services and other emergency services) and police agencies from at least ten Member States or Associated Countries in a cross- border operational setup.

On all aspects the proposal 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.

Specific requirements for the implementation of PCP are provided in the relevant Annex.

Expected impact: To create an EU interoperable broadband radio communication system for public safety and security over the next 15 years. This should lead to better services provided by first responders and police agencies with shorter reaction times, thus reducing potential casualties and/or victims.

It is expected that by delivering a European solution, the project should contribute to overcome the fragmentation of national markets and help maintaining global competitiveness of the European companies.

Type of action: Pre-commercial Procurement (PCP) - Cofund

Specific conditions related to this topic are provided along with the conditions for PCP projects in the relevant Annex.

Additional condition: Proposals should involve multiple first responders and police agencies from at least ten Member States or Associated Countries in a cross- border operational setup in phase 1 to 6 of the project. Justification for the additional condition: for this PCP to be sucessfull, it is indispensable that a significant number of police forces and/or emergency services from different Member States or Associated Countries participate to the project. The aim of this topic is to create a new EU-wide technology for public safety and security. This cannot be achieved if only a limited number of Member States or Associated Countries participate to its development.

The action is expected to proactively target the needs and requirements of public bodies and law enforcement.

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-19-2014: Communication technologies and interoperability topic 2: 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 but, for instance, making an emergency call using Voice over IP 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 emergency communication end-to-end against such requirements with each other and with the emergency services.

Scope: The proposal 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 over the internet) in a controlled-environment. It should also build a validation-focused programme/framework 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 Next Generation eCall, messaging and early warning systemsetc. The proposal should gather European technology providers, emergency services organisations, research and development laboratories, telecommunication network providers, Voice Over IP providers, and software providers to build on the expertise in a collaborative fashion.

The Commission considers that proposals requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately (similar to the Seventh Framework Programme Capability Projects described in the general introduction). 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 proposal 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.

The action is expected to proactively target the needs and requirements of public bodies and law enforcement.

The outcome of the proposal is expected to lead to development up to Technology Readiness Levels (TRL) 7; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

V. Ethical/Societal Dimension

DRS-20-2014: 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.

An insider threat particularly difficult to be timely identified is the one brought along by personnel who have undergone a violent radicalisation process that are relevant to identifying

an insider threat 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: Proposals in this area should specifically aim at strengthening the 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.

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

The proposaland the usable results should take into account 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.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposal should be directly applicable to support national and local security practitioners to strengthen the protection of national and European Critical Infrastructures from the insider threats brought by violent radicals.

In particular, the results of the proposed action are expected to contribute to an early detection of violent radicals by shedding light on the violent radicalisation processes and paths and, overall, by raising the awareness of the security practitioners about the possible early indicators that can allow a timely detection of insider threats brought to critical infrastructures by violent radicalised individuals.

The action is expected to proactively target the needs and requirements of users, such as national and local law enforcement agencies.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-21-2014: Ethical/Societal Dimension topic 2: Better understanding the links between culture, risk perception and disaster management

Specific challenge: Culture is the characteristics of a particular group of people, defined by everything from a set of values, history, literature, 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, engage in the crisis management 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.

Scope: Proposals 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, engage in restauration and recover from disaster. The gender dimension needs to be fully taken into account.

The proposal should aim at providing an analysis of existing links between disaster and culture, in particular in urban areas taking into account past and on-going EU research.

Expected impact:

- increased effectiveness of those who respond to disasters;
- a more resilient society by ensuring that cities are better prepared for and able to recover from emergencies.
- better meeting the needs of various cultures during disaster relief, thus improving reaction time and reducing fatalities;in order to provide disaster relief.
- providing a framework for improving disasters' policies and practices by taking into consideration every disaster victim's cultural and personal uniqueness.

The action is expected to proactively target the needs and requirements of users, such as citizens, first responders, urban communities and local security agencies.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DRS-22-2015: 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 aims at facilitating the adoption of a comprehensive approach, with a view to help minimising negative consequences of climate-driven crises.

Scope: Proposals 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?
- Taking into account past and on-going EU research, this topic should thoroughly examine the impact of climate-driven crises on European security.

Expected impact: This action will help stakeholders to better understand consequences of climate change events in Third Countries and its security implications for the EU.

It will provide a framework for improving situation analysis and policy planning at the EU level.

It will thus lead to earlier and better reaction of climate induced security implications by public authorities in the EU.

The action is expected to proactively target the needs and requirements of users, such as European policy makers and analysts as well as national governments.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Conditions for this call

Publication date: 11/12/2013

Deadline(s): [23] [24]

DRS - 2, 4 ,5 ,7 ,8 ,9 ,16 ,18 ,19, 20, 21 for 2014 Opening date: 25/03/2014	28/08/2014 at 17:00:00 Brussels time
DRS - 1, 3, 6, 10, 11, 12, 13, 14, 15, 22 for 2015 Opening date: 25/03/2015	(27/08/2015 at 17:00:00 Brussels time)

Overall Indicative budget : EUR 72.40 million[25] from the 2014 budget[26] and EUR 100.47 million from the 2015 budget[27]

Topics	2014 EUR million	*2015* *EUR million*
DRS - 2, 4 ,5 ,7 ,8, 16,18 ,19, 20, 21 for 2014	47.40	
DRS-9a-2014	3.00	
DRS-9b-2014	15.00	
DRS- 1, 3, 6, 12, 13, 14, 15, 22 for 2015		65.07
DRS-9-2015		15.00
DRS-10-2015		3.00

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

[24] The deadlines provided in brackets are indicative and subject to a separate financing decision for 2015

[25] This includes EUR 18 million from EUR 18 million from the societal challenge 'Climate action, environment, resource efficiency and raw materials' (budget line 08.020305) for the topics DRS-9a and DRS-9b. This also includes EUR 7 million for the SME challenge.

[26] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary authority or if the budget is not adopted as provided for in the system of provisional twelfths.

[27] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015.

DRS- 11- 2015		10.00

Eligibility and admissibility conditions:
The conditions are described in parts B and C of the General Annexes to the work programme, with the following exceptions:

DRS-6, DRS-8, DRS-9a, 18 - 2014 DRS - 6, 10, -2015;	Up to one project per year shall be funded
DRS- 5 -2014	Relevant public authorities from at least 3 Member States and Associated Countries
DRS – 18 - 2014	Proposals should involve multiple first responder and police agencies from at least ten Member States and Associated Countries 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 the relevant Annex.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in part H of the General Annexes to the work programme.

Evaluation procedure: The procedure for setting a priority order for proposals with the same score is given in part H of the General Annexes.
The full evaluation procedure is described in the relevant guide associated with this call.

- Indicative timetable for evaluation and grant agreement[28]:

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements[29]
DRS - 2, 4 ,5 ,7 ,8 ,9 ,16,18 ,19, 20, 21, for 2014	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information applicants
DRS- 1, 3, 6, 10, 11, 12, 13, 14, 15, 22 for 2015	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information applicants

Consortium agreements: In line with the Rules for Participation and the Model Grant Agreement, participants in Research and Innovation Actions or in Innovation Actions are required to conclude a consortium agreement prior to grant agreement.

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

[29] Special delay may apply following the results of the security scrutiny procedure.

Conditions for the topic: DRS 17 – 2014/2015: Critical infrastructure protection topic 7: SME instrument topic: ""Protection of urban soft targets and urban critical infrastructures "

Publication date: 11/12/2013

Opening[30]: 01/03/2014 for phase 1 and phase 2

Deadline(s) [31] [32]:

Call H2020-DRS-2014/2015 –: DRS 17 – 2014/2015 – Open call cut-off dates	Phase 1 18/06/2014 24/09/2014 17/12/2014	Phase 2 09/10/2014 17/12/2014	Phase 1 18/03/2015 17/06/2015 17/09/2015 16/12/2015	Phase 2 18/03/2015 17/06/2015 17/09/2015 16/12/2015

Indicative budget:

	2014 *EUR million*	*2015* *EUR million*
Call H2020-DRS-2014/2015 –: DRS 17 – 2014/2015	7.0 out of which 0.70 for phase 1 6.16 for phase 2 0.14 for mentoring & coaching support and phase 3	*7.40* out of which 0.74 for phase 1 6.512 for phase 2 0.148 for mentoring & coaching support and phase 3
	Single stage for both phase 1 and phase 2. The budget available for phase 1 and phase 2 will be divided equally between each cut-off date.	

Eligibility and admissibility conditions: The conditions are described in parts B and C of the General Annexes to the work programme, with the following exceptions:

Call H2020-DRS-2014/2015 –: DRS 17 – 2014/2015: [SME instrument]	Proposals for phase 1 are not required to provide a draft plan for exploitation and dissemination. A proposal for phase 2 shall include a first commercialisation plan.

[30] The Director-General responsible may delay this date by up to two months.
[31] The Director-General responsible may delay this deadline by up to two months.
[32] The deadlines provided in brackets are indicative and subject to a separate financing decision for 2015.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in part H of the General Annexes to the work programme, with the following exceptions:

DRS 17 – 2014/2015: [SME instrument]	Proposals will be evaluated individually when they arrive. They will be ranked after the respective cut-off dates. The criterion Impact will be evaluated first, then Excellence and Implementation. If the proposal fails to achieve the threshold for a criterion, the evaluation of the proposal will be stopped. For phase 1 the threshold for individual criteria will be 4. The overall threshold, applying to the sum of the three individual scores, will be 13. For phase 2 the threshold for the criterion Impact will be 4. The overall threshold, applying to the sum of the three individual scores, will be 12. The final consensus score of a proposal will be the median of the individual scores of the individual evaluators; and the consensus report will comprise a collation of the individual reports, or extracts from them. Where appropriate, a Panel Review will be organised remotely. Applicants can provide during the electronic proposal submission up to three names of persons that should not act as an evaluator in the evaluation of their proposal for potential competitive reasons[33].

Evaluation procedure: The procedure for setting a priority order for proposals with the same score is given in part H of the General Annexes.

The full evaluation procedure is described in the relevant guide associated with this call.

- Indicative timetable for evaluation and grant agreement[34]:

	Information on the outcome of the evaluation (*single stage*)	Indicative date for the signing of grant agreements
Call H2020-DRS-2014/2015 –: DRS 17 – 2014/2015: [SME instrument]	Two months after the corresponding cut-off date set out above for phase 1 and four months after the corresponding cut-off date set out above for phase 2.	One month from the date of informing applicants in phase 1 and two months from the date of informing applicants in phase 2.

[33] If any of the persons identified is an independent expert participating in the evaluation of the proposals for the call in question, they may be excluded from the evaluation of the proposal concerned, as long as it remains possible to have the proposal evaluated.

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

Consortium agreements: In the case of two or more SMEs submitting a proposal, in line with the Rules for Participation and the Model Grant Agreement, participants are required to conclude a consortium agreement prior to grant agreement.

Call – Fight against crime and Terrorism[35] [36]

H2020-FCT-2014/2015

The ambition of this call 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

Proposals are invited against the following topics:

[35] Any activity resulting from this call that manages classified information, is excluded from the delegation to REA and will be implemented by the Commission services.

[36] Some activities, resulting from this call, may involve using classified background (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification in accordance with the relevant Guide for Classification. For those activities in particular, *but not exclusively:* FCT 1, 2, 3, 5, 6, 12, proposers are invited to anticipate to the maximum extent possible the requirements for handling security sensitive information. The final decision on the classification of projects is subject to a Security Scrutiny Process. The Time To Grant will start from the completion of the Security Scrutiny Process.

I. Forensics

FCT-1-2015: Forensics topic 1: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offenses generated 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), that could be police forces and/or custom authorities, 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, GSM and GPS, can easily result in an information overload and represent a problem instead of a useful asset. In addition, we face the problem of having to deal with a huge number of cyber offenses and millions of new attack every year generating huge volume of data using obfuscation/anonymisation techniques.

Scope: Proposals 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, Data Modelling, Intelligent User's Interfaces, Information Retrieval, Weak Signal Analysis, Ontologies and Knowledge Representation. Digital intelligence capabilities should also enable smart pre-processing and filtering of sensor data and stored data in order to improve their reliability, accuracy, accessibility and transmission volume.

The scope of this topic is threefold:

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. Data exchange between LEA and network operators shall be standardized for fast and efficient processing. 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.

Thirdly, tools and platform should allow reaching a decent speed-up in the whole process of analysing cyber offenses. The main challenges are the automation of as many analysis steps as possible; the countering of the obfuscation used by the attacker and the finding an efficient way to identify an attacker despite use of anonymisation is a challenge in its own.

Proposals addressing this topic should address the three aspects of the scope and 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.

The proposal 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.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals requesting a contribution from the EU of between €9m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-2-2015. Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime

Specific challenge: Rapid developments in technologies and communication in various fields go hand in hand with new opportunities for forensic science to investigate more and a greater variety of traces, to extract more information from less material, quicker than ever before, and to keep the standards of forensic science in Europe at a high level regarding juridical and technological questions. Meanwhile, 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. .

Proposals for this topic should take into account the existing EU and national projects in this field, such as the Council Conclusions on the vision for European Forensic Science 2020 which foresee the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe."

Scope: Proposals for this topic should focus on the development methodologies of tools and EU-wide standards for the secure storage, access and the exchange of forensic data supporting evidence.

A platform integrating different techniques should be proposed in order to achieve better strategies for 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.

Specific areas of research could be:

- The establishment of a EU-wide database of new synthetic drugs and drug precursors (detection protocols and analysis methodologies).
- Other types of pan-EU databases - like for instance soils, ballistic data, breath analysis, DNA, fingerprints, 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.

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 use 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.

Proposals adressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals requesting a contribution from the EU of between €9m 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: Projects under this topic should lead to the development of novel easy to use in-situ forensic tools, customised to the specific needs of EU LEA. Better profiling of crimes and offenders. Quicker matching of different types of crime. Shorter court cases due to the availability of more solid court proof forensic evidence.

For industry better understanding of modern operational LEA requirements, thus increasing their competitiveness.

Considerable improvement in the field of public security and improved trust of the citizen in the work of police forces in the EU.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-3-2015: Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials

Specific challenge: In the event of an accident or a terrorist attack (including those involving CBRNE 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 CBRNE materials and collection of forensic material / evidence in a variety of situations and conditions.

Scope: The proposal should focus on the "mobile, remotely controlled" characteristics of the technologies to be developed 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 CBRNE 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 that they are cost effective. Proposals should link with existing projects. Tools/technologies should have a minimal disruptive effect on the crime scene.

In addition, dual-use applications will be considered with possible synergies being established with the European Defence Agency.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals requesting a contribution from the EU of between €3m 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 remotely controlled identification / detection and collection of forensic evidence in case of accidents or terrorist attacks involving CBRNE materials. Higher cost effectiveness of CBRNE forensics. For industry, better understanding of modern operational CBRNE identification/ detection requirements, thus increasing the competitiveness of their mobile equipments and products.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-4-2015: 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. Appropriate solutions to fulfil the legitimate request of privacy by the citizens should be embedded in the very core of the proposed solutions. Also, all the developed tools, methods and guidelines should be supported by training support and curricula.

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.

Proposals 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 proposals requesting a contribution from the EU of between €3m 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 LEA capabilities to conduct investigations by using information travelling and stored on the Internet obtained under a lawful warrant ;
- improved training of LEA staff able to perform these investigations. increased crime prosecution capabilities;
- shorter court cases due to the availability of more solid court proof forensic evidence;
- increased privacy and data protection during forensic investigations;
- for industry better understanding of modern operational LEA requirements, thus increasing their competitiveness.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above ; please see part G of the General Annexes.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

II. Law enforcement capabilities

FCT-5-2014: 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 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, including GSM networks) 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 and equipments, 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 and experts in

fundamental rights 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, and as experts on fundamental rights are informed on the impact of new technologies on individual lives (in particular privacy) and which rules should consequently be respected.

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

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals requesting a contribution from the EU of between €3m 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 LEA capabilities to conduct investigations by using novel monitoring systems and miniaturised sensors;
- increased crime prosecution capabilities:
- shorter court cases due to the availability of more solid court proof evidence;
- increased privacy and data protection;
- for industry better understanding of modern operational LEA requirements, thus increasing their competitiveness.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-6-2015: Law Enforcement capabilities 2: Detection and analysis of terrorist-related 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, recruitment and propaganda tool where they can safely communicate with their affiliates, coordinate action plans, raise funds, and introduce new supporters or recruits 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 finding sources of data, capturing and preserving data for forensic analysis, authenticating images and videos and conversely proving multimedia data falsification, should be investigated.

Scope: Proposals 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. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase.

The proposals should address 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 proposals requesting a contribution from the EU of between €3m 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: Projects under this topic should lead to:

- 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 activities. 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.
- Increased privacy and data protection.
- Contribution to a considerable improvement in the field of public security.
- For industry better understanding of modern operational Law Enforcement Agency requirements, thus increasing their competitiveness.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-7-2014: Law enforcement capabilities topic 3: Pan European platform for serious gaming and training

Specific Challenge:Police forces, first responders, civil security agencies and operators of critical infrastructures in the EU are constantly facing new challenges and threat scenarios. New immersive training simulations in mixed-reality environments, dynamically addressing physical threats and cyber attacks, are needed to effectively prepare and train police forces, security teams, first response units and infrastructure operators for these new situations.

Scope:Proposals should take the following aspects into account:

- incorporate high engagement, interactivity, immersion and active participation;
- non-linearity/multiple outcomes/replayability through adaptive scenarios;
- context relevant narrative game-play and interactivity with the virtual content;
- high consequences/safe failure;
- real time summative feedback; deep diagnostics and measurement functionality;
- opportunities for interoperability with other existing Sector tools and utilities;
- skills acquisition and practice including problem solving/analytical/ decision making;
- mixed-reality approach supplemented with immersive user's interface enablers (e.g. enabling use of real and/or training weapons within mixed-reality environments for enhanced realism).

The solutions would be expected to automatically generate game scenarios based on the surrounding real-life environment. Proposals for fully-immersive user interfaces enabling mixed-reality single-person and cooperative team-based training experiences, and hybrid solutions involving multiple human sensose should be explored for achieving near real experience. In addition scenarios and training material can be defined, executed and evaluated.

Proposals may address one or more areas like fighting cyber-attack for LEA, fighting Terrorist and/or Serious Crime organisation for investigators and intelligence analyst, protection of critical infrastructures, solving crisis for first responders and decision makers. The involvement of the relevant end users from the conceptual phase of this project until the testing of the final solutions is essential for all proposals.

The Commission considers that proposals requesting a contribution from the EU of between €4m and €6m would allow this specific challenge to be addressed appropriately (similar to the Seventh Framework Programme Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Research under this topic should lead to the development of training curricula, solutions and serious gaming tools for representing and modelling the environment, including computer and network systems, and the challenges and decision making processes. The results of projects stemming from this topic should be used for the training of personnel on high stress situations, very sensitive material or the challenges related to new technological evolutions.

These developed solutions should be shared among the police forces and civil security agencies of all Member States and Associated Countries.

Type of Action: Research and Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-8-2014: 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 transnational, national or regional law enforcement agencies networks in different security research domains. Activities should cover all relevant areas and additionally may focus on selected key topics. At least, this challenge should address: first, the identification of the relevant technologies for law enforcement end-users and way forward; second, the definition of a roadmap for solutions to improve interoperability of databases and information sharing systems in the area of law enforcement.

Scope: The action should further aim to:

a) exchange information on security issues in Member States and Associated Countries and define core areas of common interest in order to prevent duplication and identify synergies;

b) exchange information about identified research needs and latest technological developments to address these needs;

c) develop common strategies and mechanisms in the specific area(s); and

d) explore and demonstrate coordinated and/or joint activities (for instance in paving the way for a framework to achieve the interoperability of databases and information sharing systems, like EIXM, UMF2, SIENA, IXP and I-link).

The Commission considers that proposals requesting a contribution from the EU of between €0.5m and €1m would allow this specific challenge to be addressed appropriately If properly justified, a duration between 4 to 7 years could be proposed. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact: It is expected to improve networking, coordination and cooperation of various Member State activities targeted to security issues in the identified core area(s) at European level.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-9-2015: Law Enforcement capabilities topic 5: Identity Management

Specific Challenge:New means and technologies of communication the growing interactive usage of the internet, the rise of social media and the internet of things lead to a change in handling identity related data for law enforcement agencies and border management. These circumstances and the general digitalisation of society result in a significant qualitative and quantitative revaluation of the subject identity. As identity trust and security are central drivers for economic and societal development a framework for a reliable e-identity ecosystem needs to be set up. Such an e-ID ecosystem would safeguard the fundamental

parameters of identity management: security – efficiency – user friendliness – trust – privacy and data protection. Enhanced public security and better (digital) privacy protection will become part of the same consistent European identity strategy.

Identity Management will play a pivotal role in this system.

Identity Management starts with proper breeder documents, other identity documents including their lifecycle and goes to identification and verification for physical and virtual access as well as virtual identities in secure applications and social networks. In all these areas of identification, security is severely endangered, if identity fraud has taken place. It is very well known, that cases of identity fraud and wrong identity are heavily involved in people trafficking and organized crime. Additionally, identity fraud in virtual places leads to theft, misuse of information and cyber-mobbing. Therefore, new processes, technologies and security features needs to be developed to increase or hold the high level of quality of security documents and corresponding processes..

Scope:Technological, organizational and societal means necessary for a European electronic identity ecosystem will be identified, researched and tested:

- New security features with corresponding quality control and checking technologies
- Enhanced document lifecycle processes
- Harmonized document processes and security features
- Technologies for linking physical and virtual identity
- Combination of biometric technologies and administrative processes for identification management
- Identification of the necessary legal and societal steps to safeguard trust and data protection
- Identify patterns in identity fraud and highlight associated social networks
- Take into account and build upon results and findings of existing research projects that potentitially may contribute to an European electronic identity ecosystem

Expected impact:A European e-identity ecosystem (potentially tested on a national test-bed level) would create a decisive competitive advantage for Europe on the global level. New technologies and processes in identity management will ease the work of border management and law enforcement authorities as the identity verification becomes more reliable. The personal security increases dues to reduced risk of identity fraud and cyber mobbing. Finally, improved id documents will make people trafficking and organized crime more difficult. A European e-identity ecosystem should make use of existing research results in this field to the highest possible extent to optimise funding impact.

Type of action: Research and Innovation Actions

III. Urban security

FCT-10-2014: Urban security topic 1: Innovative solutions to counter security challenges connected with large urban environment

Specific Challenge: European large urban environments are subject to various challenges and threats to urban security linked to their big size and large population. 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 to prevent, mitigate and recover from the above-mentioned security challenges and to foster their 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 architecture, 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 security and privacy 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. Strong synergies may be expected in the fields of 3D mapping, accurate positioning and timing services, GIS analysis functions and environment modelling, simulation and visualisation technologies.

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

The Commission considers that proposals requesting a contribution from the EU of between €3m 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:

- Reduce the fear of crime and enhance the perception of security of the inhabitants of large urban environments.
- Better addressing security challenges in large urban environments.
- Increase the perception of security of citizens by empowering them, fostering their sense of belonging to a greater community.
- Facilitating the engagement of citizens to improve the security conditions of smart cities.
- Providing new market opportunities, especially for SMEs and entrepreneurs, to develop and produce innovative technologies for urban security.

The action is expected to proactively target the needs and requirements of users, such as citizens and local police forces.

The outcome of the proposal is expected to lead to development up to Technology Readiness Levels (TRL) 5; please see part G of the general Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-11-2014: Urban security topic 2: Countering the terrorist use of an explosive threat, across the timeline of a plot, including the detection of explosives in a flow

Specific challenge: Extensive research has been undertaken in recent years to enhance support to those involved in detecting and countering explosive threats. This research should propose innovative approaches to develop methods/technologies able to fill existing gaps or greatly improve already existing along the terrorist timeline, 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, and in particular in a flow of vehicles / people;
- Neutralizing the IED and undertaking forensic and evidential work.

Furthermore, a substantial amount of research and development has been carried out for other purposes, that could be applied to efforts to counter IEDs and Home-Made Explosives (HMEs). For instance, federated sensors are being developed to detect air/water pollution in sewages, streets and buildings.

But up to now, no comprehensive research was undertaken to assess the effectiveness, the efficiency and the cost of all the developed methods/techniques (including those initially designed for a different purpose). Detecting an explosive threat inside a flow of vehicles or passengers (including carried bags) also remains a major challenge at the present day.

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.

Scenarios should take into account the type of explosive (e.g. home-made, conventional) and the means of transit and deployment (e.g. person-borne, vehicle-borne, left baggage), as both of these factors will have an influence on how effective a given combination of methods/technologies will be.

On detection in transit, projects should focus on the optimal combination of several existing technologies, for example spectroscopic stand-off detection; active/passive imaging for hidden objects detection; dogs (or other animals); automated CCTV tracking; multi-sensor data treatment. It should also cover the best way to locate sensors, taking into account realistic operational conditions and past event scenarios. In addition, technologies should be developed to fill identified detection gaps, such as e.g. bio-inspired technologies, stand-off-eye-safe spectroscopy, tomography, radar imaging, polarimetry etc.

In addition, the proposal should identify the weakness of the current defences on IED and the best candidates to make them better.

The Commission considers that proposals requesting a contribution from the EU of between €3m 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:
- Better understanding of the effectiveness of the supporting method/technology used to counter the terrorist use of an explosive threat.
- Allowing 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 technologies.
- Better understanding of the combination of technologies required to detect and locate an explosive threat inside a flow, providing security and police forces with enough information so that they are able to take quick and effective decisions.
- Contribution to a considerable improvement in the field of public security.

The outcome of the proposal is expected to lead to development up to Technology Readiness Levels (TRL) 7; please see part G of the general Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-12-2014 Urban security topic 3: Minimum intrusion tools for de-escalation during mass gatherings improving citizens' protection

Specific challenge:Mass gatherings, especially in urban environments, have a potential risk of escalation and therefore may pose a threat to the safety of humans and the security of the society. LEA representatives as well as people in the crowd and in the neighborhood are

regularly injured, sometimes seriously, during the course of such events. Hitherto approaches of LEAs for de-escalation often lack the capabilities to defuse rising tensions with minimal intrusion techniques.

Research is needed to identify, test and assess new means of protecting citizens in crowd environments deteriorating into aggresive scenarios or even riots, such as sound, smell, communication, etc.. These means should be administered locally and with high precision in places where crowd parameters are reaching critical values regarding the safety of citizens. Crowd management tactics that are based on containment and controlled break-up by force could be replaced by festival tactics where one or more disrupting elements are removed with high precision and minimum intrusion before large scale escalation happens.

This can only be done if crowd management instruments are improved significantly with new sensors and processing capabilities. A strong societal dimension component should be at the core of the legal and ethical rules of operation as a prerequisite to ensure the acceptance of citizens of the instruments.

Scope:The proposals should aim to develop novel technological tools for public order management to help LEAs protect citizens while de-escalating public unrest (especially in cases of influence by alcohol and/or drugs). These tools should be altogether efficient and harmless and could use, for example lights, noise or scents. They should also: enable to focus on a specific group or a single individual inside a crowd; be difficult to counter; and have minimum to none impact on bystanders.

The proposal should include the largest possible number of LEA representatives in the consortium.

Expected impact:The project should help to protect citizens by developing minimum intrusion and efficient tools in order to prevent escalation and severe injuries and casualties. The results of the proposals should lead to the elaboration of more effective and less intrusive police actions that significantly reduce the risk of escalation during mass gatherings and increase the level of urban security and its perception among the citizens.

Type of Action: Research and Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

IV. Ethical/Societal Dimension

FCT-13-2014: Ethical/Societal Dimension Topic 1: Factors affecting (in-) security

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 proposal, taking into account past and on-going EU research, should be based on real life examples and address factors affecting the perception of personal (individual) (in)security as well as (in)security perception in spontaneous and more structured groups. Furthermore, this action should aim at collecting and analysing data assessing the elements that influence individual and the group's perception of (in)security. 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: The project should aim at:

- Elaborating a number of priority areas and suggestions for policy makers in order to improve the perception of security within targeted groups.
- Identification of different factors influencing public (group) and personal (individual) assessment of (in)security.
- Improving overall strategic security policy making.
- Better understanding of how demographic background influences the feeling of (in)security.

The action is expected to proactively target the needs and requirements of users, such as security planners and policy makers working at different levels.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-14-2014: 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: Proposals 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 as well as EU prevention policies, are expected to analyse "community policing" as an opportunity to use a community to observe their environment identify risk and exchange information. This concept based on collaboration and coordinated activities should be analysed as a system aimed at facilitating information sharing and trust building. To this end, the proposed research should also take into account the virtual dimension of “community policing” (i.e. the interaction between

citizens and police officers through social networking websites) and analyse its underlying social, cultural, legal and ethical dimensions. The proposal should aim to develop 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.Citizen or community representatives should be actively engaged in the research, to ensure that their perspectives are well embedded in the design of new technology and innovation.

In addition to the above, proposers should focus on trainings for law enforcement agents (for instance by means of serious games or simulations), as well as on awareness raising activities about community policing, for both police and citizens. These activities should also take the gender dimension into account. The Commission considers that proposals requesting a contribution from the EU of between €2m and €5m would allow this specific challenge to be addressed appropriately (similar to the FP7 Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact: Strengthened community policing principles through effective and efficient tools, procedures and approaches.

Early identification, timely intervention, as well as better crime reporting, identification of risks, unreported and undiscovered crime through the community.

Strengthened and accelerated communication between citizens and police forces. Overall, strengthened community feeling and lower feeling of insecurity.

The action is expected to proactively target the needs and requirements of users, such as citizens and national and local law enforcement agencies.

The outcome of the action is expected to lead to development up to Technology Readiness Levels (TRL) 6; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-15-2015: Ethical/Societal Dimension Topic 3: Better understanding the role of new social media networks and their use for public security purposes

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 attention from public security planners.

Scope: This topic shall look at the role and purpose of social media and the relationship between the new social networks and public security. Research to be coordinated by this activity may focus on analysing the following issues:

- To what extent are social media likely to influence public security planning?
- Shall the adoption of social media across the public security community be treated as a threat or a tool for public security purposes?

- Shall the potential of social networking tools be explored by public security agencies for example in order to predict future trends or identify possible threats?

Special attention should be paid to ethical and privacy aspects.

Expected impact: Better understanding among research organisation across Europe: of how social media can be used for public security purposes, in particular for better prediction and identification of possible future threats, and of the challenges, opportunities and risks for public security agencies of using social media. .

The action is expected to proactively target the needs and requirements of users, such as law enforcement agencies, citizens and public security planners.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-16-2015: Ethical/Societal Dimension Topic 4 - Investigating the role of social, psychological and economic aspects of the processes that lead to organized crime (including cyber related offenses), and/or terrorist networks and their impact on social cohesion

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. Where appropriate, research should also take into account the potential impact of organized crime on social cohesion of societies.

Research on the human and economic factors in (cyber) crime has not kept pace with research and innovation regarding its technological dimensions. Yet, while the latter may be able to defuse a threat, it does not tackle its causes and remedies. The research needs to address a human and economical point of view in addition to a technological focus. By taking multi-disciplinary approaches, integrating the social, economical and technological sciences a new light is shed on the human factor in (cyber) crime. Proposers of projects seeking to understand cyber-crime should be cognizant of this emphasis.

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 could cover short- mid- and long term trends pertaining to the impact of organised crime and terrorist networks on societal vulnerabilities. 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 could 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 proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately (similar to the FP7 Capability Projects described in the general introduction). Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

In line with the EU's strategy for international cooperation in research and innovation[37] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

Expected Impact:

- Better understanding of the origins and development of organised crime and terrorist networks;
- Better understanding of 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;
- Where appropriate to the project, give insights for policy makers at different levels (regional, national, European, international) into ways to improve social cohesion.

The action is expected to proactively target the needs and requirements of users, such as policy makers at different levels (regional, national, European and international).

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

FCT-17-2015: Fast track to Innovation Topic

It is noted that the following information is provided at this stage only to facilitate the familiarisation with this topic. The Commision will provide in due course full details, together with the announcement of the relevant calls, on the Fast track to Innovation Topic.

The general aspects of this topic are as follows:

[37] COM(2012)497

Under this Fast Track to Innovation (FTI) pilot, proposals for innovation actions linked to any technology field will be invited, on the basis of a continuously open call (with its first cut-off date in 2015) and a bottom-up-driven logic.

Any legal entity may participate and proposals may be submitted at any time. The Commission shall initiate three cut-off dates per year to evaluate proposals. Time between a cut-off date and signature of the grant agreement or notification of the grant decision shall not exceed six months. No more than 5 legal entities shall participate in an action. The amount of the grant shall not exceed EUR 3 million.

Proposals shall be ranked according to the impact, quality and efficiency of implementation and excellence, with the criterion of impact given a higher weighting. Factors such as time sensitivity and the international competitive situation shall be taken into sufficient account when evaluating the impact of a proposal, to allow for flexibility according to the various specificities within different fields of applied research.

Conditions for this call

Publication date: 11/12/2013

Deadline(s): [38] [39]

FCT - 5, 7, 8, 10, 11, 12 13, 14 for 2014 Opening date: 25/03/2014	28/08/2014 at 17:00:00 Brussels time
FCT- 1, 2, 3, 4, 6, 9, 15, 16, 17 for 2015 Opening date: 25/03/2015	(27/08/2015 at 17:00:00 Brussels time)

Indicative budget : EUR 34.81 million from the 2014 budget[40] and EUR 44.26 million from the 2015 budget[41]

	2014 EUR million	*2015* *EUR million*
FCT - 5, 7, 8, 10, 11, 12 13, 14 for 2014	EUR 34.81 million	
FCT - 1, 2, 3, 4, 6, 9, 15, 16, 17 for 2015		EUR 44.26 million

Eligibility and admissibility conditions:
The conditions are described in parts B and C of the General Annexes to the work programme, with the following exceptions:

FCT-8-2014	This topic is limited to public end-users. Additionally proposals should contain at least 7 public authorities from different Member States and Associated Countries and or international law enforcement organisations. Justification for the additional condition: the central aim of this topic is to bring together a high number of public end-users in the field of security

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

[39] The deadlines provided in brackets are indicative and subject to a separate financing decision for 2015

[40] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary authority or if the budget is not adopted as provided for in the system of provisional twelfths.

[41] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015

	research. It is therefore essential that a critical mass of public authorities participate to a proposal for this topic.
FCT-8, FCT-11 -2014	Up to one project per year shall be funded

Evaluation criteria, scoring and threshold: The criteria, scoring and trshold are described in part H of the General annexes to the work programme.

Evaluation procedure: The procedure for setting a priority order for proposals with the same score is given in part H of the General Annexes.
The full evaluation procedure is described in the relevant guide associated with this call.

- Indicative timetable for evaluation and grant agreement[42]:

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements[43]
FCT- 5, 7, 8, 10, 11, 12 13, 14 for 2014	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information of the applicants
FCT- 1, 2, 3, 4, 6, 9, 15, 16, 17 for 2015	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information of the applicants

Consortium agreements:
In line with the Rules for Participation and the Model Grant Agreement, participants in Research and Innovation Actions or in Innovation Actions are required to conclude a consortium agreement prior to grant agreement.

[42] Should the call publication be postponed, the dates in this table should be adjusted accordingly.
[43] Special delay may apply following the results of the security scrutiny procedure

Call – Border Security and External Security[44] [45]

H2020-BES-2014/2015

On the one hand this call targets the development of technologies and capabilities which are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security. This includes 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. It also addresses supply chain security in the context of the EU's customs policy.

On the other hand this call focuses on new technologies, capabilities and solutions which are required to support the Union's external security policies in civilian tasks, ranging from civil protection to humanitarian relief, border management or peace-keeping and post-crisis stabilisation, including conflict prevention, peace-building and mediation. This will require research on conflict resolution and restoration of peace and justice, early identification of factors leading to conflict and on the impact of restorative justice processes.

This call is divided in the following parts:

- Maritime Border Security
- Border Crossing Points
- Supply Chain Security
- Information Management in the context of External Security
- Conflict Prevention and Peace Building
- Ethical/Societal Dimension

Proposals are invited against the following topics:

[44] Any activity resulting from this call that manages classified information, is excluded from the delegation to REA and will be implemented by the Commission services.

[45] Some activities, resulting from this call, may involve using classified background (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification in accordance with the relevant Guide for Classification. For those activities in particular, *but not exclusively:* BES 4, 9, proposers are invited to anticipate to the maximum extent possible the requirements for handling security sensitive information. The final decision on the classification of projects is subject to a Security Scrutiny Process. The Time To Grant will start from the completion of the Security Scrutiny Process.

I. Maritime Border Security

BES-1-2014: Maritime Border Security topic 1: radar systems for the surveillance of coastal and pre-frontier areas and in support of search and rescue operations[46]

Specific challenge: The challenge refers to early and distance border surveillance. Research is needed in the development of Over the Horizon (OTH) radars of improved performance, reduced cost, lower power requirements, deployable. Deployability is an important issue, also because of its impact on the coastal environment and of public alarms that bulky radar installations may provoke. 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. The validation work package should involve public authorities and be foreseen in a realistic SAR operational scenario.

The Commission considers that proposals 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 research is expected to contribute to redress the limitations of current border surveillance systems at sea, particularly concerning the detection and tracking of small unseaworthy vessels. Impact will be benchmarked against improved capabilities to meet surveillance requirements in conditions ranging from those of the Southern Atlantic to the Greek archipelago. The dimension of the challenge is shown in the discrepancy which may occur between the attributed areas where maritime surveillance and rescue operations shall be provided and the available resources of the concerned countries.

This topic would contribute further to the development of the European Border Surveillance System (EUROSUR) and the Common Information Sharing Environment (CISE) at sea. 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[47], 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. For this reason all Iinnovations shall be able to seamlessly cooperate and interface with existing infrastructure supporting the CISE constituent communities. The appropriate participation of competent national authorities should be a prerequisite for the implementation of this project."

Type of action: Innovation Actions

[46] For this topic specific rules related to Article 25.5 "Option 1*"* and Article 31.5 "Option 4" of the model grant agreement may apply.

[47] 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 drugs.

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-2-2015: 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 or other relevant technologies provide promising results for the detection of targets in areas that cannot be covered by active systems. Passive radars fit this application, due to electromagnetic invisibility, lower detectability and cost and the possibility of use practically anywhere.

R&D is needed to better apply this technology maritime surveillance, also in combination with other systems, and using the signals coming from existing 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 proposals requesting a contribution from the EU of between €3m 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 impact of the research will be benchmarked against the potential for integration of novel technology into current border surveillance systems in order to redress its limitations. This topic would contribute further to the development of the European Border Surveillance System[48] (EUROSUR) and the CISE. Innovations shall be able to seamlessly cooperate and interface with existing infrastructure supporting the CISE constituent communities.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

[48] 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 drugs.

BES-3-2014: Maritime Border Security topic 3: Light optionally piloted vehicles (and sensors) for maritime surveillance[49]

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. In addition, the analysis of current operational obstacles faced by the End-Users community shows that weaknesses in communications capabilities (in particular related with tactical communications, interoperability and standardization) hinder the detection, identification and tracking of small boats at the external EU Maritime borders. The tactical communications between surface and aerial assets are considered to be a key for improving situational awareness, early warning and reaction capacity.

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 and to improve the communication between assets, which is particularly critical in multi-national joint operations, where different systems co-operate in one single operational scenario (to be tested in the context of a real operational scenario, such a Frontex led joint operation).

Scope: The proposal should cover technologies for surveillance (e.g. low weight/high performance radar and electro-optic/systems and hyperspectral sensors) for the detection and early identification and tracking of moving targets (e.g. with moving target indication and data fusion/correlation capabilities), as well as methods for obstacle detection and avoidance and technologies that improve naval platforms performances for surveillance . It should take into account the exchange of real time data with any martitime/aerial asset no matter where the operation is conducted and independently from the existing surveillance infrastructure. Research should take into consideration the maritime surface segment in the communication with aerial assets in order to accommodate tactical communication technologies. These technologies could also be useful for the detection of marine pollution incidents. The research could also cover innovative designs in naval architecture and marine engineering, for platforms (crafts, small boats) to accommodate such technologies. The innovative crafts should present high efficiency/low operational costs profiles, and possibly contribute to standardisation in construction.

The fitness for purpose of novel solutions should be validated using affordable, optionally piloted, reconfigurable aerial and/or naval platforms (compliant with current regulations) connected with ground control stations, as in legacy surveillance systems, and designed in order to be fit also for installation in optionally piloted aircrafts and/or RPAS (Remotely Piloted Aerial System), when regulation will allow.

The appropriate participation of competent border authorities should be a prerequisite for the implementation of this project.

The Commission considers that proposals 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.

[49] For this topic specific rules related to Article 25.5 "Option 1" and Article 31.5 "Option 4" of the model grant agreement may apply.

Expected impact: The impact of the research shall be measured in terms of cost-effectiveness and efficiency of the proposed systems (to be tested in quasi-operational scenarios) as compared to more conventional border surveillance systems. This topic would contribute further to the development of development of the Common Information Sharing Environment (CISE) at sea initiative and the concept of Common Application of Surveillance Tools, contributing not only to the development of joint communications capabilities, but also to the enhancement of the mobility, projection and sustainability of a common pan-European pool of maritime border patrol equipment, as included in the final steps of the European Border Surveillance System[50] (EUROSUR).

These technologies developed could, in addition, also be used to support the detection of marine pollution incidents.

Type of action: Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-4-2015: 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. It is a global issue, addressed in particular by the Mini Dublin Group of the UN. As an example, this situation has been identified as a major gap to combat drug smuggling entering through the south coast of Spain and Portugal.

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,runways, or even roads and landstrips, which makes the early detection of these aircrafts crucial to determine the landing area.

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

1. Identification of technological gaps in already operational systems, including those used by the military, and in cooperation with responsible authorities.
2. Mobile units which can be quickly deployable in remote areas with communication links with command and control centres.
3. Multi-mode radar technologies for the early detection, target pre-classification and tracking of low flying aircrafts.

[50] 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.

4. Integration of radar data and correlation with repositories of information to predict most probable landing areas.
5. New type of sensors that could be deployed at low cost increasing the detection and narrowing the grid of detection. The solutions proposed should consider the employment of technologies enabling multi-functionality and miniaturization of the hardware components.

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.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

In line with the EU's strategy for international cooperation in research and innovation[51] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

Expected impact: This topic would contribute further to the development of the European Border Surveillance System[52] (EUROSUR)

The impact of the research shall be measured in terms of increased capabilities to contribute to the prevention of cross border crime, in particular in terms of reduction of the traffic of drugs, weapons and illicit substances. Its outcome should complement the surveillance tools (and strategy) being used at present.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

II. Border crossing points

BES-5-2015: 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.

[51] ***COM(2012)497***

[52] 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 drugs.

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 that could (or could not) be combined with border authorities dedicated mobile equipment to perform identity checking for border security.

A general challenge is to make the technical equipment affordable enough to be widely employed.

Scope: Studies 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. The approach to use technology from adjacent markets such as mobile or satellite telecommunications, where the volumes of production are very high, could help the costs of processing down to a minimum. 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 to be further improved. 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 considered 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 proposals 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: 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. Harmonization of requirements across Member States and Associated Countries (and standardization) is expected to also automatically greatly improve affordability. The outcome of the research should be assessed in terms of contribution to meeting such challenges.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-6-2015: 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 are being 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, the 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, of 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 bona-fide 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 facial picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and could be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. 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 the 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. The 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 proposals requesting a contribution from the EU of between €3m 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 and Associated Countries 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. The outcome of the research should be assessed in terms of potential to improve border management and control modalities facilitating travel without compromising security. The expected impact is to make the daily work of border control authorities more efficient and to significantly facilitate bona-fide non-EU citizens in crossing EU external borders.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-7-2015: Border crossing points topic 3: 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 supposed to support border authorities in carrying out border control and surveillance tasks, and (c) a 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. A general challenge is to make the equipment and procedures more appropriate for wide employment. A further general challenge that applies to all scenarios is interoperability (operational as well as technical).

Scope: Studies 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 and procedures that are user friendly and reliable in operational conditions.

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 operators with new technologies (e.g., through simulations, virtual environments), and (c) designing optimal information workflows for particular border control scenarios to avoid disproportionate burden on EU external border control authorities and economic operators/citizens, (i.e., which information to utilize and fuse with other, and which to discard, with a view to address the threats in the most efficient manner and at the best place (e.g. in the logistical chain of goods flows)) etc. The underlying data to support the decision making and/or planning in the context of such tool could come from past information gathered over longer period of time.

Expected impact: The outcome of the research should be assessed in terms of improved border control modalities with a view to dedicate more time and resources to identify those who may pose a threat. The expected impact is to make the daily work of border control authorities more efficient and to significantly facilitating non-EU citizens and goods/economic operators in crossing EU external borders.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

III. Supply Chain Security

BES-8-2015: 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 may be narcotics, explosives, currency and weapons and could also be ampoules containing chemical and biological threats. All these items 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 are expected to 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 the challenge, and so assist development in proposals which may be for either a sub category or for a combined solution.

1) Internally concealed commodities

Packages may be ingested, or inserted into body orifices. Ingested packages may be formed of compressed powder, or even liquid and may weight 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 were to utilise ionising radiation, it would have to comply with European limits of dose. It should also be noted that not all Member States and Associated Countries permit use of ionising radiation for non-medical purposes.

2) Externally concealed commodities.

Packages such as drugs can be concealed beneath clothing and even be 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 or Police/Security interest from harmless items and alert the operator. 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). The privacy of individuals must be respected.

The Commission considers that proposals 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.

In line with the EU's strategy for international cooperation in research and innovation[53] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

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;
- to significantly improve security at the border;
- to constitute an effective tool against organised crime;
- to lead to increased crime prosecution capabilities;
- to lead to increased privacy and data protection.

The impact of the research should be benchmarked in terms of future deployment, as proportionate to the risks being assessed, and taking into account realistically the expected improvements in performance, functional needs, conditions of use, future maintenance costs, and impact on operating procedures, including training requirements for new skills.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 5; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-9-2014: 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.

[53] COM(2012)497

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.

Scope: 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.

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

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.

It is difficult to predict a priori which technology will yield the most practical solution. Therefore, 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). The solutions proposed should address the employment of innovative technologies, which have been demonstrated to be able to dramatically enhance the performance of imaging and sensor systems.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. 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 proposals 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.

In line with the EU's strategy for international cooperation in research and innovation[54] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops, and US homeland security research entities. Funding for third countries is however still subject to the evaluations.

[54] COM(2012)497

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. 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. As the research should facilitate and expedite the smooth flow of legitimate international trade through improved security controls, it would support the work of WCO for high risk cargo.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 7; please see part G of the General Annexes.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

IV. External Security

BES-10-2015: Information management topic 1: Civilian humanitarian mission personnel tracking

Specific challenge: Civilian intervention staff in humanitarian missions is 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. Their security is of a paramount importance.

Scope:Proposals should address the problem of tracking (from the headquarters) the assets and the staff of the missions deployed in third countries for instance in the CSDP context. Real-time tracking may help to reduce the exposure to security risks of these missions. The proposed solution should integrate and/or complement seamlessly the communication system in use (either standard or specific) and, if any, the Control and Command system in place (even if abroad). It must integrate features to assure its own security not being usable if in wrong hands. It should also integrate navigation/guidance (in the field) of assets and staff, using European GNSS where appropriate. Cost effectiveness should be considered (both acquisition and operation) as clients are quite often NGOs with limited resources.

The Commission considers that proposals requesting a contribution from the EU of between €3m 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 project should lead to the development of novel secure communication and tracking solutions/technologies for civilian missions, in particular those of the European External Action Service. Through better tracking of civilian intervention staff it should lead to more efficient and effective humanitarian missions. Ultimately, it should reduce threats to personnel on the ground and contribute to a more efficient implementation of such missions.

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-11-2014: Information management topic 2: Information management, systems and infrastructure for civilian EU External Actions[55]

Specific challenge: Considering the range of civilian CSDP missions in complex environments, the ability to efficiently manage information and resources is a key factor to enhance decision-making, planning and conduct capabilities and to increase the efficiency, visibility and impact of those actions in all the phases of crisis management, from early warning up to "the-lessons-learned' phase. There is a need to identify the state of the art of the existing processes, procedures, equipment (information management systems and infrastructures, tools, technologies), cultures, within the context of the EU External Action with a view to developing a coherent and interoperable situational awareness and information exchange capability to improve decision-making, planning and conduct related to EU external action and crisis management operations.

The development of a Situational Awareness, Information exchange and Operation Control Platform will improve cooperation among different EU actors and with Member States and Associated Countries, with the possibility to involve also other international organisations, and in particular EU partners in crisis management, notably UN, NGOs, etc.. The needs of decision-makers, planners and 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, Information Exchange and Operation Control Platform.

Based on a stocktaking of the existing system, the activity is expected to focus on the definition of services, interfaces, formats and protocols for sharing selected objects of relevance consumed or produced by the entities involved in EU external actions. Focus should be on interoperable, secure, resilient communication services to be deployed and shared by the entities involved . The action will lead to the specifications of a platform demonstrator where existing systems will be plugged in. This platform should address EU actions decision-makers, planners and end-users needs following the cycle decision-action-information. This platform to be developed may lead to a PCP project in the future.

The Commission considers that proposals requesting a contribution from the EU of between €1m and €2m 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 activity should lead to the creation of a strong community of interest for EU civilian external actions. Additionally, the selected proposal should develop key research priorities and thus pave the way for a demonstrator, which should be entirely focused on the needs of the decision-makers, planners and the end-users. The envisaged platform should allow all stakeholders to enhance their common understanding of crisis management in EU civilian external actions. It should also improve the management of the EU resources' allocated to combatting crisis and help federating the Community of Interest (CoI) amongst entities involved.

[55] For this topic specific rules related to Article 25.5 "Option 1*"* and Article 31.5 *"*Option 4*"* of the model grant agreement may apply.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-12-2014: Conflict prevention and peace building topic 1: Enhancing the civilian conflict prevention and peace building capabilities of the EU

Specific challenge: Since the end of the cold war the relative global political stability created through the balance of power between the Soviet Union and the US has considerably decreased. Across the world the new multipolar structure of international politics reopened dormant conflicts and lead to new emerging crisis situations.

Overcoming these new conflicts necessitates novel approaches on prevention, mediation and peace keeping to which the occidental world is only insufficiently prepared. Classical stabilisation/intervention operations are often not appropriate anymore, nor do they guarantee any long term stability. Conflicts cannot be overcome solely by military or civilian means alone.

The majority of these conflicts are asymmetrical by nature. This often implies that the primary victims are non-combatants, particularly in civil wars. The humanitarian crises (famines, epidemics, forced migrations) that follow often affect especially women and children. These conflicts represent both a humanitarian obligation for the EU to act, and a liability for the external and internal security of the EU. Economic and political disparities have often proven to be a breeding ground for political extremism, violent radicalisation and terrorism.

These geopolitical changes and challenges are reflected in the articles 42-46 on the Common Security and Defence Policy (CSDP) of the Treaty on European Union: "*the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation."*

Scope: Research in this field should focus on :

- Analysing past and on-going civilian and military efforts of the EU, its Member States, Associated Countries and international organisations (UN, OSCE) on conflict prevention and peace building in and between third countries.
- Assessing the potential for pooling and sharing of capabilities and technologies for civilian conflict prevention.
- Research should go beyond the short term stabilisation/conflict prevention and focus on long-term peace building by civilian means.
- A catalogue of best practices and lessons learned should be developed in the form of a living document.
- Identifying research priorities on civilian conflict prevetion for Horizon 2020 security research.
- Special attention should be paid to civilian-military synergies on an operational level.

Expected impact: Projects resulting from this topic should develop a clear assessment of the capabilities of the EU for external conflict prevention and peace building and identify the best civilian means to enhance these capabilities.

A set of clear policy priorities and technological needs on civilian conflict prevention should be developed, with a focus on the exploitation of civilian-military synergies.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

BES-13-2015: Conflict prevention and peace building topic 2: Training curricula for Conflict Prevention and Peace Building personnel

Specific challenge: Over the last ten years, the Commission has become increasingly active in the field of Conflict Prevention and Peace Building (CPPB). This involvement is likely to further increase over the years to come and a more extensive use of the articles 42 to 46 on the Common Security and Defence Policy (CSDP) of the Treaty on European Union.

Scope: Projects under this proposal should develop new training methods in the field of civilian conflict prevention and peace building such as: conflict prevention, mediation, Security System Reform (SSR), Linking Relief, Rehabilitation and Development (LRRD), anti-corruption, early warning systems, etc.

Expected impact: New training curricula for enhancing the preparedness and skills of personnel for conflict prevention and peace keeping missions especially in high risk countries. Thus contributing to more efficient and effective conflict prevention and peace keeping missions. Ultimately, this should reduce the costs of such missions, whilst at the same time contribute to a more efficient implementation of the CSDP.

Type of action: Coordination and Support Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

V. Ethical Societal Dimension

BES-14-2014: 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;

- compare and agree a match or non match between the facial image in the passport with the face of the traveler, irrespective of ethnic background, age difference or normality in the passport image.

Scope: Studies 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.

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. 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 proposals 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 research should make a major contribution in improving the effectiveness of EU border control. It will 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.

The action is expected to proactively target the needs and requirements of users, such as border management decision-makers, border guards and citizens (regular travellers).

Type of action: Research & Innovation Actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Conditions for this call

Publication date: 11/12/2013

Deadline(s)[56] [57]:

BES- 1, 3, 9, 11, 12, 14 for 2014 Opening date: 25/03/2014	28/08/2014 at 17:00:00 Brussels time
BES- 2, 4, 5, 6, 7, 8, 10, 13 for 2015 Opening date: 25/03/2015	(27/08/2015 at 17:00:00 Brussels time)

Indicative budget : EUR 40.78 million from the 2014 budget[58] and EUR 20.09 million from the 2015 budget[59]

	2014 EUR million	*2015* *EUR million*
BES- 1, 3, 9, 11, 12, 14 for 2014	EUR 40.78 million	
BES- 2, 4, 5, 6, 7, 8, 10, 13 for 2015		EUR 20.09 million

Eligibility and admissibility conditions:
The conditions are described in parts B and C of the General Annexes to the work programme, with the following exceptions:

BES-11 - 2014	Up to one project per year shall be funded

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in part H of the General Annexes to the work programme.

[56] The Director-General responsible may delay this deadline by up to two months.
[57] The deadlines provided in brackets are indicative and subject to a separate financing decision for 2015
[58] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary authority or if the budget is not adopted as provided for in the system of provisional twelfths

[59] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015

Evaluation procedure: The procedure for setting a priority order for proposals with the same score is given in part H of the General Annexes. The full evaluation procedure is described in the relevant guide associated with this call.

- Indicative timetable for evaluation and grant agreement[60]:

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements[61]
BES - 1, 3, 9, 11, 12, 14 for 2014	Maximum 5 months from the final date for submission	Maximum 4 months from the date of information of the applicants
BES - 2, 4, 5, 6, 7, 8, 10, 13 for 2015	Maximum 5 months from the final date for submission	Maximum 4 months from the date of information of the applicants

Consortium agreements:
In line with the Rules for Participation and the Model Grant Agreement, participants in Research and Innovation Actions or in Innovation Actions are required to conclude a consortium agreement prior to grant agreement.

[60] Should the call publication postponed, the dates in this table should be adjusted accordingly.
[61] Special delay may apply following the results of the security scrutiny procedure

Call – Digital Security: Cybersecurity, Privacy and Trust

H2020-DS-2014/2015

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; fundamental rights protection; norms of behaviour). The proposed activities in this domain address the economic and societal dimension of security and privacy 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 and increasing the trust in 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 Call will thus focus on demonstrating the viability and maturity of state-of-the-art security, privacy and trust solutions that have been tested in a laboratory environment. The intention is 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.

However, there is still a large number of unresolved cybersecurity, privacy and trust issues that necessitate longer term research. Constantly new questions come up due to the evolution of ICT or the usage made thereof. Digital security is an issue cutting across all ICT technology, components, applications or services. Generic research is thus needed addressing those more fundamental and ubiquitous questions. Therefore, this call is complementary to the Cybersecurity and Trustworthy ICT activities supported under the "Information and Communnication (ICT)' theme of the 'Leadership in Enabling and Industrial Technologies' (LEIT) pillar of H2020 where those longer term issues are addressed.

Proposals are invited against the following topics:

DS-1-2014: Privacy
Specific challenge: Many online users are 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 often includes the use of data they collect (e.g. social networks, search engines, online retailers, and cloud hosting services).

Data protection and privacy frameworks in Member States and Associated Countries need to be implemented in a transparent and user-friendly way to help users understand how their personal data might be used, including the economic value of their data. Such knowledge will enable them to exercise choice and know and assert their rights. As the economic value of their data is not known to the average user, they are not able to evaluate the value of their data relative to the value they assign to a "free" service. Moreover, the users have no control over what happens with their data, e.g. they cannot verify the data is not passed on to 3rd parties. This situation may influence individuals notion of privacy which may be perceived as a non-valuable asset.

Data protection principles need to be visibly respected for the delivery of personalised public services, to increase trust in public administrations. Transparency is particularly important in an open government context, where personal data may be shared between different departments and administrations or across borders and where third parties can engage in the creation and delivery of personalised services for citizens and businesses.

Scope: The focus is on the demonstration of solutions to protect individuals' privacy by default while empowering the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving them control over how their data will be used by service providers (including public authorities), and making it easier for them to verify both whether their online rights are respected and if they get a reasonable bargain. The activities may also cover tools facilitating the information of individuals about the processing of their personal data. Systems will either have to detect the privacy settings automatically, or the data will have its privacy settings permanently associated to it by the user.

Activities can include the investigation of measures to safeguard privacy in the context of mass data handling, for example where 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.

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

Expected impact: The actions supported under this objective are to provide a practical, user friendly and economically viable implementation of the legal obliations related to personal data processing and the legal obligation for prior consent. The actions will not only identify but more importantly implement privacy by design architectures. It is expected that the actions will lead to an increased user trust online, resulting in a higher uptake of online services. Actions should generate positive business cases for online privacy.

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS-2-2014: 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 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.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €8m EURO would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact: Actions supported under this objective will deliver secure, but user-friendly, access to ICT systems, services and infrastructures, resulting in a consumerisation of devices for access control. The level of security of online services and critical infrastructures protected by these access systems should be demonstratably higher than by the state-of-the-art approach. The proposed solutions are expected to support the creation of commercial services making use of electronic identification and authentication.

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS-6-2014: Risk management and assurance models

Specific challenge: The ability to assess, manage, reduce, mitigate and accept risk is paramount for an effective protections against cybersecurity threats and incidents. 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.

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[62] public-private platform (Network Information Security Platform) will seek to identify best practices on risk management, including information assurance, risks metrics and awareness raising.

[62] ***JOIN (2013)1***

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. Where necessary risk management can include ICT supply chain security.

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.

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

Expected impact: A risk management framework has to be put in place allowing the comprehensive comparison between sector specific or national approaches, and providing an assessment on the residual risk. The framework will facilitate the implementation of legal obligations on risk management, identify gaps in existing legislation, while remaining adaptive to possible changes in the legal frameworks[63].

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS-3-2015: 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.

This includes Industrial and Automation Control Systems (IACS). They are no longer isolated siloes but are fully integrated with corporate IT infrastructures. Despite this strong connection between the two infrastructures, there is only little awareness regarding IT risks that can affect

[63] In particular such as the European Union's proposal for a Directive on Network and Information Security

IACS. An attack to IT assets can spread to the OT environment jumping to SCADA and Control Centres.

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 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 (including SCADA and IACS systems) of critical infrastructures, analyze and propose mitigation strategies and methodologies for assessing criticalities of services and detecting anomalies, developing tools and processes to simulate or monitor cascading effects due to ICT incidents, 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.

In relation to the protection of legacy IACS, SMEs are particularly encouraged to provide specific and very focused security solutions adapting current ICT security technology to IACS environments on topics such as:

- Early anomaly detection and compliance management.
- Patching and updating equipment without disruption of service and tools.
- Improved forensic techniques for supporting criminal law enforcement.
- Anti-malware solutions with special focus on managing third-parties (e.g. maintenance and support service providers, IACS vendors, etc.)

The Commission considers that proposals requesting a contribution from the EU of between €3m and €8m EURO would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

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. Reduced possibilities to misuse ICT as a vehicle to commit cybercrime or cyber-terrorism. Where relevant, the supported activities should support the work of the European Program for Critical Infrastructure Protection (EPCIP).

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS-4-2015: Secure Information Sharing

Specific challenge: To protect our society and economy against accidental or man-made disruptions of the information and communication technologies they so much depend on an efficient exchange of information on vulnerabilities, incidents or attacks is desirable. However, at the moment the private and public stakeholders 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. The NIS[64] public private platform (Network Information Security Platform) will discuss, among other things, best practices on information sharing and incident coordination. Inputs from other cooperation networks will also be used.

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 between for example market operators, nationalauthorities, law enforcement agencies, business sectors, SMEs or citizens. 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 private and public authorities such as EC3, CERT's, ENISA, 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.

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

Expected impact: The pilots will establish an operational information sharing between the stakeholders, public or private , building trust between the stakeholders and develop practical incentives for information sharing. The actions are expected to lead to a faster response to incidents and/or vulnerability through faster sharing of information and an enlarged source of information. Ultimately the actions will reduce the impact of incidents and in particular increase the level of preparedness of all stakeholders, public or private, and in particular

[64] JOIN (2013)1

SMEs. The pilots should facilitate the implementation of legal obligations on risk management, identify gaps in existing legislation, while remaining adaptive to possible changes in the legal frameworks.

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS-5-2015: 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.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €8m EURO would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

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, accessing social networks, or accessing the services of local or national administrations (e.g. issuing documents like driver's licence, visa, …). 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..

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Conditions for this call

Publication date: 11 December 2013

Deadline(s)[65] [66]:

DS-1,2,6 for 2014	13 May 2014 at 17:00:00 Brussels time
DS-3,4,5 for 2015	[21 April 2015] at 17:00:00 Brussels time

Indicative budget : EUR 47.04 million from the 2014[67] and EUR 49.61 million from the 2015 budget [68]

	2014 EUR million	*2015 EUR million*
DS- 1-2014	19.04	
DS- 2-2014	18.00	
DS- 6-2014	10.00	
DS- 3-2015		17.50
DS- 4-2015		15.31
DS- 5-2015		17.50

Eligibility and admissibility conditions:
The conditions are described in parts B and C of the General Annexes to the work programme.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in part H of the General Annexes to the work programme.

Evaluation procedure: The procedure for setting a priority order for proposals with the same score is given in part H of the General Annexes. The full evaluation procedure is described in the relevant guide associated with this call.

[65] The Director-General responsible may delay this deadline by up to two months.
[66] The deadlines provided in brackets are indicative and subject to a separate financing decision for 2015
[67] The budget amounts for 2014 are subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary authority or if the budget is not adopted as provided for in the system of provisional twelfths..
[68] The budget amounts for 2015 are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015..

- Indicative timetable for evaluation and grant agreement[69]:

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements
DS- 1, 2, 6 for 2014	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information applicants
DS- 3, 4, 5 for 2015	Maximum 5 months from the final date for submission	Maximum 3 months from the date of information applicants

Consortium agreements: In line with the Rules for Participation and the Model Grant Agreement, participants in Research and Innovation Actions or in Innovation Actions are required to conclude a consortium agreement prior to grant agreement.

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

Other actions [70] [71]

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

New satellite navigation applications are being developed every day, covering numerous sectors of the economy, hence increasing drastically the dependency of an important part of the economy on such technology.

The Public Regulated Service (PRS) is one specific objectives of the Galileo programme. This PRS service is restricted to government-authorised users, for sensitive applications which require a high level of service continuity. The purpose is therefore to develop the demonstrations and pilot projects allowing to benefit from the security related characteristics of this service to a large number of new applications. This work will entail use and production of classified information and technologies.

These Horizon 2020 activities are complementary to the funding of the infrastructure and the operations of the EGNSS, which will come from the budget of the Regulation of the European Parliament and of the Council on the implementation and exploitation of European satellite navigation systems. In addition, full complementarity with the space part in leadership in enabling and industrial technologies will be ensured. The space part concentrates on the development of enabling technologies for PRS.

Activities on two specific actions will be funded from the Security budget through public procurement actions with a maximum budget of € 20 million.

The implementation of these procurement activities will be entrusted to the European GNSS Agency (GSA) on the basis of article 58(1)(c) of the Financial Regulation. The GSA will manage all the phases of the project life cycle. To this end, a delegation agreement will be concluded between DG Enterprise and Industry and the GSA setting out in detail the entrusted tasks. The GSA has been chosen taking into account the experience acquired from the implementation of similar Galileo security related projects in FP7, its expertise in the field of security, in-line with its regulatory tasks and the Decision 1104/2011 of the European Parliament and the Council.

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

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 PRS 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

[70] The budget amounts for 2014 are subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary authority or if the budget is not adopted as provided for in the system of provisional twelfths

[71] The budget amounts for 2015 are indicative and will be subject to a seperate financing decision to cover the amounts to be allocated for 2015

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 prototype for a demonstrator in 2016.

The research shall focus on the following points:

- Develop a PMR receiver combined with PRS (following PRS4PMR demonstrator);
- Security certification and accreditation; and
- Provide logistic support and training.

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 (no framework contract will be used)

Indicative timetable: 2014

2 - PRS item 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 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 and validation of its security;
- Detailed definition of internal and external interfaces;
- Development, assembly and integration of the different elements;
- Qualification testing and associated verification activities; and
- Acceptance testing and accreditation.

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

Type of Action: Public procurement – one single contract (no framework contract will be used)

Indicative timetable: Second quarter of 2015

3 - Space surveillance and tracking (SST)

In its proposal (*COM (2013)107 final*) for "establishing a space surveillance and tracking support programme (SST)", it is foreseen that the H2020 will contribute to the funding of the SST support programme will be partly supported by Horizon 2020, since R&D activities for better space surveillance are part of the Horizon 2020 Specific programme.

This action specifically aims (1) at supporting the pooling national resources on the SST objectives outlined in COM (2013) 107 and coinciding with objectives and challenges of H2020 related to protecting Europe's investment made in space infrastructure, and (2) at achieving significant economies of scales by adding related H2020 resources to this joint effort, instead for the Commission to implement its own specific activities.

A consortium of beneficiaries is expected to be established further to consultation with the Council, to implement the SST support programme at European level.

Type of action: Identified beneficiary

The standard evaluation criteria, thresholds, weighting for award criteria and the maximum rate of co-financing for this type of action are provided in parts D and H of the General Annexes.

Indicative budget: EUR 1.2 million

Indicative timetable: 2015

4 - 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. Furthermore, this action should be complementary to the activities funded by DG HOME on ERNCIP.

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

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

The standard evaluation criteria, thresholds, weighting for award criteria and the maximum rate of co-financing for this type of action are provided in parts D and H of the General Annexes.

Indicative budget: EUR 0.25 million for 2014 and 0.25 for 2015

Indicative timetable: 2014-2015

5 - Developing Law Enforcement Tools and Techniques in the Fight Against Cybercrime
European law enforcement agencies require more sophisticated tools to investigate and combat cybercrime. The methods of cybercriminals to carry out and conceal their illicit activities continually evolve and necessitate an effective response also on the technological level. Cybercriminal activities to be targeted include the theft of identity and intellectual property, online scams such as phishing, spoofing and pharming, scareware and ransomware, content-related crime including child sexual abuse and other forms of organised crime carried out online (e.g. extortion, money laundering, fiscal fraud).

The action will be carried out through public procurement procedures, open to all eligible entities as per the rules of H2020. The entire budget will be made available to third entities, with no H2020 budget used for the administration. Specific procurement activities will focus on development of tools and techniques for understanding and disrupting cybercriminal activity. In this respect close alignment will be done with work on emerging Information and Communication Technologies (ICT) in the H2020 LEIT Program. These activities will aim procuring source and test tools and technologies for use by cybercrime investigators and at enabling the development of tailor-made tools and techniques for investigations. Assessing the performance of working prototypes and test products in an operational environment will enable Europol to align product development with end-user priorities, at a point where it is still possible to influence industry roadmaps and upcoming standards. Results, tools and technologies will be made available by Europol to Member States' cybercrime units across the EU at low or no cost.

The implementation of these procurement activities will be entrusted to Europol on the basis of article 58(1)(c) of the Financial Regulation. Europol will manage all the phases of the project life cycle. To this end, a delegation agreement will be concluded between the European Commission and Europol setting out in detail the entrusted tasks. The European Cybercrime Centre (EC3) within Europol gathers the most advanced expertise needed at EU-level. The first procurement procedures will be launched in 2014, with a view to concluding contracts with a maximum duration of 30 months.

Cybercrime subjects to be covered include:

- tools and software for the gathering of digital evidence, adapted to cloud storage, 'darknets', other emerging technological solutions and evolving mobile communications;
- tools and software to track digital money flows used for criminal transactions;
- tools and software for the analysis and investigation of cybercriminal tools, such as botnets and malware.

The tools will take into consideration emerging ICTs, notably cloud and the Internet of Things.

Type of Action: Public Procurement – a maximum of three single contracts will be used (no framework contract will be used)

Budget: 2.00 million in 2015.

Indicative timetable: within the year 2015.

6 – Evaluations of the proposals for the 2014 and 2015 calls "Disaster-resilience: safeguarding and securing society, including adapting to climate change", "Fight against crime and terrorism" 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: Expert contracts

Indicative budget: Up to EUR 0.85 million from the 2014 budget and EUR 1.15 million from the 2015 budget

7 – External expertise - Evaluations of the proposals for the 2014 and 2015 calls "Digital Security: Cybersecurity, Privacy and Trust"

This action will support the use of appointed independent experts for the evaluation of project proposals and, where appropriate, for the monitoring of running projects.

Type of action: Expert contracts

Indicative budget: Up to EUR 0.7 million from the 2014 budget and EUR 0.75 million from the 2015 budget

8 - 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.

c) Organisation of cybersecurity conferences and support to other cybersecurity events; socio-economic studies, impact analysis studies and studies to support the monitoring, evaluation and strategy definition for the cybersecurity policy of DG CNECT.

Type of action: Public procurement. It is expected to sign up to 5 direct service contracts, and up to 10 specific contracts under 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 for points a) and b); up to EUR 1.2 million from the 2014 and from the 2015 budget for point c)

9 - Ex post evaluation of the FP7 Security Theme[72]

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: Public Procurement (a framework contract[73] will be used)

Indicative timetable: fourth quarter 2014

Indicative budget: EUR 500.000 from the the 2014 budget

[72] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies is excluded from the delegation to REA and will be implemented by the Commission services.
[73] ENTR/Ì72/PP/2012/FC - LOT 4

Budget – SC7 Secure societies

Calls	**2014**[74] **Budget EUR million**[75]	*2015*[76] *Budget EUR million*
Call H2020-DRS-2014/2015 Disaster-resilience: safeguarding and securing society, including adapting to climate change	54.40[77] *from 02.040302*	*65,07*
Call H2020-FCT-2014/2015 Fight against crime and Terrorism	34.81 *from 02.040302*	*44.26*
Call H2020-BES-2014/2015 Border Security and External Security	40.78 *from 02.040302*	*20.09*
Call H2020-CP-2014/2015 Digital Security: Cybersecurity, Privacy and Trust	*47.04 from 09.040303*	*49.61*
Other Actions	**2014**[78] **Budget EUR million**[79]	*2015*[80] *Budget EUR million*
Experts (expert evaluators, experts groups, monitors)	*0,85 from 02.040302 0,70 from 09.040303*	*1,15 from 02.040302 0,75 from 09.040303*
Subscription	N/A	N/A
Pre- identified beneficiary		*1.2 (SST consortium)*

[74] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary ~~a~~authority or if the budget is not adopted as provided for in the system of provisional twelfths.

[75] The budget figures given in this table are rounded to two decimal places.

[76] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015.

[77] To which EUR 18 million from the societal challenge 'Climate action, environment, resource efficiency and raw materials' (budget line 08.020305) will be added making a total of EUR 72.40 million for the call 2014 and EUR 28 million from the societal challenge 'Climate action, environment, resource efficiency and raw materials' (budget line 08.020305) will be added making a total of EUR 100.57,77 million for the call 2015. This include EUR 7 millions (2014) and EUR 7,4 millions (2015) for the SME challenge.

[78] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary ~~a~~authority or if the budget is not adopted as provided for in the system of provisional twelfths.

[79] The budget figures given in this table are rounded to two decimal places.

[80] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015.

	0.25 (for JRC) from 02.040302	*0.25 (for JRC) from 02.040302*
Public procurement -	*10.00 (GSA) from 02.040302* *0.50 (ex post FP7 evaluation) from 02.040302* *0,90 (workshops) from 02.040302* *0.58 (workshops) from 09.040303*	*10.00 (GSA) from 02.040302* *2.0 (EUROPOL) (incl. 1.5 from 02.040302 and 0.5 from 09.040303)* *1,00 (workshops) from 02.040302* *0.63 (workshops) from 09.040303*

Horizontal activities (08.020501)	**2014**[81] **Budget EUR million**[82]	*2015*[83] *Budget EUR million*
Dissemination activities (see Part 17 of the work programme)	0.16 *of which 0.12 from 02.040302 and 0.04 from 09.040303*	*0.17* *of which 0.13 from 02.040302 and 0.04 from 09.040303*
Corporate communication (see Part 17 of the work programme)	0.09 *of which 0.07 from 02.040302 and 0.02 from 09.040303*	–

Estimated total budget	191,06	196.18

[81] Subject to the availability of the appropriations provided for in the draft budget for 2014 after the adoption of the budget for 2014 by the budgetary ~~a~~uthority or if the budget is not adopted as provided for in the system of provisional twelfths.

[82] The budget figures given in this table are rounded to two decimal places.

[83] The budget amounts are indicative and will be subject to a separate financing decision to cover the amounts to be allocated for 2015.