ANNEX 17 TO THE DECISION

SECOND DRAFT VERSION

DRAFT

WORK PROGRAMME 2016 – 2017

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

(European Commission C(2015)XXX of XX XXXXX 2015)

Table of contents

Explanatory preliminary notes 5

CALL – CRITICAL INFRASTRUCTURE PROTECTION 6

CIP - CIP 1 - 2016 and 2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe. 6

CALL – SECURITY 10

Sub Call - Disaster-resilience: safeguarding and securing society 11

SEC - DRS 1 - 2016: Integrated tools for response planning and scenario building 12

SEC - DRS 2 - 2016: CSA on situational awareness systems to support civil protection preparation and operational decision making 14

SEC - DRS 3 - 2016: Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control 16

SEC- DRS 4 - 2017: PCP of broadband communication systems 18

SEC - DRS 5 – 2016 - 2017: CBRN cluster 20

Sub Call – Fight against crime and Terrorism 22

SEC - FCT 1 - 2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection 23

SEC - FCT 2 – 2016 – 2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts. 25

SEC - FCT 3 - 2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA 27

SEC - FCT 4 - 2017: PCP of toolkits integrating tools and techniques for forensic laboratories 29

SEC - FCT 5 - 2017: Integration of detection capabilities and data fusion with utility providers' networks 31

SEC - FCT 6 - 2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot 33

SEC - FCT 7- 2016 - 2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism. 34

DRAFT

Sub Call – Border Security and External Security....36

SEC – BES 1 – 2017: PCP of next generation of information systems to support EU external policies....37

SEC - BES 2 – 2016: Towards reducing the cost of technologies in land border security applications....39

SEC - BES 3 – 2017: Risk-based screening at border crossing....41

SEC - BES 4 – 2017: Through-foliage detection, including in the outermost regions of the EU....43

SEC - BES 5 – 2017: Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements....45

SEC - BES 6 – 2017: Acceptance of "no gate crossing point solution"....47

SEC - BES 7 - 2016: Data fusion for maritime security applications....49

SEC - BES 8 – 2016: Autonomous surveillance with enhanced command and control systems for the surveillance of borders in a 3D environment....51

Sub Call - General Matters....53

SEC – GM 1 – 2016 and 2017: Pan European Networks of practitioners and other actors in the field of security....54

SEC – GM 2 – 2016 and 2017: SME Instrument....59

SEC – GM 3 – 2016 Fast track to Innovation – Pilot....59

CALL – DIGITAL SECURITY....60

DS1 – 2016: Cyber Security for SMEs, local public administration and Individuals....61

DS2 – 2016: Economics of Cybersecurity....63

DS3 – 2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation....65

DS4 – 2017: Addressing Advanced Cyber Security Threats and Threat Actors....67

DS5 – 2017: Privacy and Data Protection and Digital Identities....69

Sub Call – Digital Security and SMEs....71

SMEInst-XX -2016-2017: Innovative European SMEs in cybersecurity....71

OTHER ACTIONS (NOT SUBJECT TO CALLS FOR PROPOSALS)....72

1 - Space surveillance and tracking (SST)....72

2 - Supporting the implementation of the Security Industrial Policy and Action Plan through the European Reference Network for Critical Infrastructure Protection (ERNCIP)....72

3 – Evaluations of the proposals for the 2016 and 2017 calls "Critical Infrastructure Protection" and "Security"....74

DRAFT

4 – Evaluations of the proposals for the 2016 and 2017 calls "Critical Infrastructure Protection" and “Digital Security”.....74

5 - Support to workshops, conferences, expert groups, communications activities or studies 74

DRAFT

Explanatory preliminary notes

Note on the meaning of the "Impact" section:

The better the specific impacts mentioned can be delivered from a project, the higher the mark of the proposal in respect to the "Impact" criteria

Note on the meaning of "Conditions for the topic/eligibility criteria":

All conditions stated under this section must be satisfied by the proposals, or they will be declared not eligible

Note on the formatting:

The formatting of this document may change once the IT support tool for drafting work programs becomes available. For the time being some short phrases/questions and tick boxes are used, that will be replaced by text on due time.

Note on "special modalities" for PCP of H2020 SC7:

A new text is being prepared in interaction with representatives from industry.

Note on "Budgetary indication for proposers":

When a "Budgetary indication for proposers" is indicated, it refers to the envisaged amount of the EC contribution ***per project***.

Note on "Practitioner participation mandatory":

When the mention: "Practitioner participation mandatory" is accompagnied with minimum participation requirements (eg: '3 LEA from 3 different MS or AC), the condition refers to full membership in the consortium.

Note on "Possible classification":

All topics will be subject to security scrutiny.

DRAFT

CALL – CRITICAL INFRASTRUCTURE PROTECTION

CIP - CIP 1 - 2016 and 2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

Specific challenge:

Disruptions in the operation of our countries' infrastructure may put at risk the functioning of our societies and their economies. Such disruptions may result from many kinds of hazards and physical and/or cyber-attacks on installations and systems. Recent events demonstrate the increased interconnection between the two kinds of attacks and, conversely, the usefulness for operators to combine cyber and physical security-solutions to protect installations of the critical infrastructure of Europe: A comprehensive, yet installation-specific approach is needed to securing the integrity of existing or future, public or private, connected and interdependent installations. Since the global financial crisis has imposed unprecedented budgetary restrictions on both the public and private sectors, new security solutions must be more efficient and cost-effective than the ones currently available.

Scope:

Proposals should focus on one of the following critical infrastructures: Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means of transportation, Communication Infrastructure, Health Services, Financial Services.

Proposals should cover: prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs) over the life span of the infrastructure, with a view to achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment. They should not only address in details all aspects of both physical (e.g. bombing, plane or drone overflights and crashes, spreading of fires, floods, seismic activity, etc.) and cyber threats and incidents, but also systemic security management issues and the combinations of physical and cyber threats and incidents, their interconnections, and their cascading effects. Innovative methods should be proposed for sharing information with the public in the vicinity of the installations, and the protection of rescue teams, security teams and monitoring teams.

Expected impact:

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.
- Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure
- Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.
- Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the infrastructure.
- In situ demonstrations of efficient and cost-effective solutions.

DRAFT

- Security risk management plans integrating systemic and both physical and cyber aspects.
- Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.
- Where relevant, testbeds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protections, against prevailing standards and guidelines
- Test results and validation of models of a specific critical infrastructure against physical and cyber threats.
- Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.
- Convergence of safety and security standards, and the pre-establishment of certification mechanisms.
- Contributions to relevant sectorial frameworks or regulatory initiatives.

General aspects of the topic

Innovation Action

Budgetary indication for proposers: about 8 MEUR per action. Two to 3 actions to be financed for this topic in 2016, and another 2 to 3 in 2017.

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

TRL level: 7

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐ : At least 2 operators of the chosen critical infrastructure operating in 2 countries must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement.

The participation of industry is required.

SME participation mandatory: yes ☒ / no ☐

Other specific eligibility criteria

A maximum of one project will be selected per critical infrastructure listed in the "Scope" section of this topic over the 2016-2017 period.

Only the installations not covered in 2016 will remain eligible in 2017. A list of topics that remain eligible in 2017 will be published in due time.

DRAFT

CONDITIONS FOR THIS CALL

Publication date:
Deadline:

Indicative budget:

	2016 EUR million	*2017* *EUR million*	
Topics:	]	----------	*All single stage*
Topics	----------		*All single stage*

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

Evaluation criteria:

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

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

- Proposal page limits and layout: 120 pages [TBC]
- Indicative timetable for evaluation and grant agreement[1]: *[as appropriate]*
  - *specify planned date to inform applicants of outcome of evaluation, and.*
  - *indicative date of signature of grant agreements or notification of grant decision*

	Information on the outcome of the evaluation (*single or first stage*)	Indicative date for the signing of grant agreements

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

Topics: ,	XX	XX
Topics:	XX	XX

Consortia agreements: *[as appropriate]*

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

DRAFT

CALL – SECURITY

DRAFT

Sub Call - Disaster-resilience: safeguarding and securing society

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

DRAFT

SEC - DRS 1 - 2016: Integrated tools for response planning and scenario building
Specific challenge:

At present, the wide range of sectors, disciplines and actors involved in disaster risk management are not sufficiently interlinked, which prevents efficient response planning and the building of realistic multidisciplinary scenarios. Integrated tools need to be developed to support such actions. Stronger partnerships among research, policy, (research or monitoring) institutes, industry/SMEs communities and practitioners, in particular first responders, are required for better preparedness of societies to cope with complex crisis situations.

Scope:

Disaster risks (natural, accidental, or intentional) should be addressed in the context of:
- the EU Civil Protection Mechanism (Decision 1313/2013), which paves the way for reinforced cooperation in civil protection assistance interventions for the protection primarily of people, and also of the environment and property in the event of natural and man-made disasters, emergency situations in case of mass events, acts of terrorism and technological, chemical, biological, radiological or environmental accidents;
- the IPCC[2] recommendations in relation to extreme climatic events;
- the Sendai Framework for Action at international level.

Response to emergency situations resulting from the materialization of such risks requires inter-organisational coordination among many actors, and efficient coordination requires improved response planning and scenario building. This can only be achieved through the integration of support tools that can be used operationally by a large variety of decision-makers, back-office experts, and first responders. Such tools can build upon previous and ongoing FP7 projects and preliminary results from H2020 actions to avoid duplication, and should be demonstrated in representative and realistic environments and situations involving firefighting units, medical emergency services, police departments, and civil protection units.

Expected impact:
- More efficient response capacity of the EU in particular in the frame of the "request for assistance" mechanism
- Improved strategy for response planning and scenario building in the EU and beyond (in particular in the context of the Sendai Framework for Action)
- Enhanced autonomy, mobility (i.e. long range, quick deployment) and resilience of rescue and first aid organisations in case of natural or man-made disasters, including in remote regions or in case of emergency situations during mass events
- Updated knowledge of existing relevant capabilities, and of best practices and lessons learned from similar, past incidents
- Enhanced understanding of human factors in relation with events affecting critical infrastructure
- Development of new tools, and adaptative networking of existing technologies (e.g. self-deploying infrastructure and autonomous sensors including passive sensors early warning systems, satellite-based integrated monitoring, system networks for recovery) that are useful for response planning and scenario building, including e.g. modular concepts and systems based on renewable energies, robust and flexible autonomous systems for transport and rescue missions, electric vehicles, emergency aircraft load planning optimization, mobile power

[2] Intergovernmental Panel on Climate Change

DRAFT

systems, new resilient electrical energy storage systems, mobile laboratories, autonomous system entities (land- and air-based) etc. using data exchange standards, demonstrating a high level degree of interoperability, the ability to be used in all-hazards approaches (man-made and natural disasters, and their combination), and compliant with EU guidelines and recommendations

- Development of scenarios developed in specific geographical areas with the direct involvement of local authorities and end-users
- Development of novel visual interfaces and user-friendly tools enhancing stakeholders and population awareness and involvement
- Enhanced cooperation between autonomous systems entities: satellite-, sea-, land- and air-based systems, including but not limited to the Copernicus, Galileo and EGNOS systems, from different agencies and of a large variety of capabilities, and costs
- Assessment of the societal acceptance of such tools, also from an ethical point of view.
- Greater cooperation among actors involved in crisis management
- Stronger involvement of practitioners (e.g. first responders and monitoring institutes) in validating and testing of tools, concepts and methodologies

General aspects of the topic

Innovation Action

Budgetary indication for proposers: about 8 MEUR per action. No more than 2 actions to be financed for this topic

International cooperation: yes ☒ / no ☐

TRL level: TRL 7 or 8

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐ : At least one entity from each of the 5 following categories of first responders must participate in any proposal: firefighting units; medical emergency services; police departments; civil protection units; control command centres

SME participation mandatory: yes ☒ / no ☐

DRAFT

SEC - DRS 2 - 2016: CSA on situational awareness systems to support civil protection preparation and operational decision making

Specific challenge:

A major difficulty for civil protection actors to take proper, coordinated decisions for efficient actions (in relation with prevention, preparedness, surveillance, and in particular: response in times of crisis) results from insufficient situational awareness. This is even truer in the context of the EU Community Civil Protection mechanism[3]: reinforced cooperation across borders calls for improved cross-border situational awareness.

Technologies close to maturity and prototype tools exist, that gather or provide data and information from a wide variety of sources useful to improve situational awareness in time of crisis. But no system that satisfactorily integrates these technologies and tools, and fuse these data and information, is available yet. Additionally, there is a theoretical framework which should be focused to understand the psychological, cultural, language and societal dimension of situational awareness in order to prevent, prepare and manage crisis situations

Scope:

Situational awareness systems for EU, national, regional and local buyers should be cost effective and interoperable, integrate different technologies (sensors; sub-systems for surveillance, early warning systems, communication systems, satellite-based systems), result from public-private cooperation, and demonstrate resilience and relative self-sufficiency.

Situational awareness systems need to be customizable by specific civil protection authorities, and adaptable to various risks and crisis scenarios (for instance: climate-related hazards, industrial accidents, earthquakes, biohazards, space weather events, etc.), especially in the context of cross-border cooperation.

The action will identify new and promising solutions, develop and agree on the core set of specifications of a specific system, on the roadmap for research still needed for its development, and the related tender documents upon which to base future (research services and system) procurements.

The EU may contribute to subsequent actions (PCP, PPI, other types of funding, …) aiming at implementing tender procedures to develop, test and validate prototypes of such a system.

Expected impact:

- Improved cooperation among civil protection services across the EU and Associated Countries
- Improved cooperation between hazard-monitoring institutes and civil protection services
- Improved exchange of experiences amongst (public) stakeholders on civil protection in relation to operations within the disaster risk management cycle (prevention, preparedness, surveillance, response);
- Improved European humanitarian Enhanced Response Capacity
- Lower operating costs for European humanitarian actions

Further to the CSA's successful achievement, the European Commission may consider calling for a PCP/PPI co-fund action in the future.

[3] Decision 1313/2013

General aspects of the topic

Coordination and Support Action

Budgetary indication for proposers: yes ☒ / no☐: about 1.5 MEUR per action, No more than 1 action to be financed for this topic

Only one project to be financed for this topic?: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

TRL level: 6 for techniques and tools to be considered, and 8 for the envisaged prototype situational awareness system

Conditions for the topic/eligibility criteria

The proposals must necessarily state the participants' commitment to make the standards, specifications, and all other relevant documents generated in the action available at actual cost of reproduction to any law enforcement or first responder organization established in an EU or EEA country.:

To ensure that the outcome of the action becomes also available to non-participating Member State organisations for further capability or product procurement purposes, the proposals must necessarily state the:

1. Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to use the result of the action to run a procurement process, and solely for that purpose.
2. Commitment from participating procurement authorities to involve the action beneficiaries in the decision on which information to release, for the purpose set out in paragraph 1.
3. Commitment from participating procurement authorities to negotiate the use granted under paragraph 1 on fair, reasonable and non-discriminatory (FRAND) terms.

DRAFT

SEC - DRS 3 - 2016: Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control

Specific challenge:

Recent incidents in Europe and worldwide recalled that biological toxins can be produced by laypersons and intentionally released in a criminal act to harm people. While different technologies are available for toxin detection and analysis, recent findings have shown that the comparability of analytical results from different laboratories is poor, which cast severe doubts about the validation of current methods and about the overall validity of analytical data. This means that in case of a bioterrorist act using compounds such as e.g. ricin, saxitoxin, botulinum, neurotoxins, enterotoxins, etc. there is no guarantee that decisions to react are made based on data meeting basic quality requirements. The lack of quality assurance/quality control tools (e.g. certified reference materials of ricin, botulinum, etc.) and standard operating procedures hampers the validation and the EU-wide comparability of biological toxin measurement data. There is therefore a need to develop an EU-wide approach for enhancing validating analytical capacities for biological toxin measurements in case of bioterrorism threats, similarly to what exists regarding chemical threats.

Scope:

By their characteristics, biological toxins are in between the classical chemical (C-) and biological (B-) toxins, and are covered both by the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). The large variability among families of biological toxins complicates their measurement and unambiguous identification in human specimens, and environmental or food samples. Toxins are rapidly metabolised and degraded after incorporation, limiting the time window for successful identification and forensic analysis. Proposals should develop quality control tools, as well as the Standard Operating Procedures necessary for establishing a mechanism to systematically validate laboratory-based measurement techniques, including sample preparation strategies and analyses made in-situ issued by mobile and quickly deployable laboratories, which should be proposed for adoption at EU level.

Expected impact:

- Development, production and certification of reference materials for biological toxin determinations as a basis for strengthened validation capacities;
- Establishment of a stepwise learning inter-laboratory programme enabling control laboratories to improve their analytical skills and development and testing of an European Proficiency Testing (EPT) scheme from sampling to detection;
- Improved capabilities for the validation and testing of existing and emerging techniques, including sample preparation strategies, mobile laboratories for in-situ analyses and technical approaches for forensic analysis, for the detection and identification of biological toxins;Replacement of old "gold standards" employing animal experiments with death as endpoint for detection of potent biological toxins, by modern, in vitro methods as requested by EU regulations;
- Based on the outcome of the EPT scheme, development of Standard Operational Procedures for the validation of analytical techniques, including in-situ techniques for biological toxin determinations in human specimens, environmental and food samples.

General aspects of the topic

Innovation Action

DRAFT

Budgetary indication for proposers: about 8 MEUR per action. No more than 1 action to be financed for this topic

Possible classification: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no ☐ : At least 3 control laboratories from different Member States or Associated Countries

DRAFT

SEC- DRS 4 - 2017: PCP of broadband communication systems

Specific challenge:

So far each EU Member States has adopted its own (broadband) radio-communication system for security forces (police, first responders, etc.). Such systems are not necessarily compatible with each other. The EU has funded projects to help to overcome this issue, including a CSA (under Call DRS-18-2015) for buyers of such systems to develop the core set of specifications and tender documents to be used for national procurements, or the legal setting of alternate organisational solutions which remain to be implemented taking into account the requirements for interoperable next generation PPDR broadband communication systems.

Scope:

If the above-mentioned CSA has foreseen to go along the way of establishing a new organization intended for taking EU-wide responsibilities a short Phase 0 may be needed:

Phase 0: Legal establishment of the new organization, and transfer of the PCP contract from the consortium of buyers to this new organization.

If the above-mentioned CSA does not foresee the need for establishing a new organization, Phase 0 will be skipped, and the PCP would start with:

Phase 1: Plan and implement the tender procedures, based on the set of specifications and tender documents delivered by the CSA launched under Call DRS-18-2015, for procuring:

- prototype communication equipment's that will constitute the foreseen communication system
- prototype instruments for validating the components of the foreseen communication system

Phase 2: Establishment of a (networked) validation centre equipped with these instruments. 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.

Phase 3: Testing and validation of the prototype components of the foreseen communication system

Phase 4: Demonstration of the foreseen communication system in a multidisciplinary (firefighters, police departments, medical emergency services, etc.), international (involving practitioners from at least 10 Member States or Associated countries), and realistic scenario.

Expected impact:

Established EU-interoperable broadband radio communication system for public safety and security, providing better services to first responders and police agencies and allowing shorter reaction times to prevent from casualties or victims, deployed by 2025.

For this impact to be as large as possible across the EU, special conditions have been attached to the CSA launched under Call DRS-18-2015 as regards access to standards, specifications, and all other relevant documents.

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: about 10 MEUR per action. No more than 1 action to be financed for this topic

TRL level: 8

Conditions for the topic/eligibility criteria

If Phase 0 is necessary, proposals must involve buyer organizations from at least 12 EU Member States

If Phase 0 is not necessary, proposals must involve buyer organizations from at least 8 EU Member States

To ensure that the outcome of the PCP action becomes also available to non-participating Member State organisations for further capability or product procurement purposes, the proposals must necessarily state the:

1. Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product fully or partly derived from the PCP action the use of the information required to run such a procurement process, and solely for that purpose.

2. Commitment from participating procurement authorities to involve the PCP beneficiaries in the decision on which information to release, for the purpose set out in paragraph 1.

3. Commitment from participating procurement authorities to negotiate the use granted under paragraph 1 on fair, reasonable and non-discriminatory (FRAND) terms.

DRAFT

SEC - DRS 5 – 2016 - 2017: CBRN cluster

Specific challenge:

Technologies and innovations in the field of CBRN are developed by SMEs or larger companies which often face difficulties in bringing them to markets: because they address local, small niche markets; or because these SMEs have neither the capabilities nor the strategic objective to go for foreign markets; or because the individual technologies that they develop can make it to the market only if integrated and combined with other tools by other companies that have the capabilities and the strategy to market its products abroad, and possibly on the global market.

Such synergies among companies are not frequent in the area of CBRN technologies, which is to the detriment of industrial competitiveness, and which limits considerably the offer made to the practitioners if one compares with the actual technological state-of-the-art.

Scope:

A CBRN cluster could articulate two kinds of actions:

Part a) (2016): A CSA supported by a complementary grant will gather the largest number of European companies capable and willing to market their products globally (e.g. companies producing integrated equipment for First Responder's, CBRN software systems, detectors, decontaminators, waste management and encapsulation equipment). The participants in the CSA will provide platforms (toolkits and systems in the field of CBRN) in which to integrate the technologies and innovations developed by other companies under Part B). Building upon the inventory developed an dmade public by the EDEN project (EDEN store), the CSA will issue a catalogue of technologies that need to be developed with a view to integrating them into the platforms. The CSA will deliver the first version of the catalogue on time for use in the implementation of Part b). The participants in the CSA will provide commercial and other services enabling access to the global market for the results of the RIA selected for support under Part b). The CSA will report publicly on its discussions, and assess and provide feedback on the impact of the business deals implemented with the research and innovation activities led by SMEs under Part b) of this topic.

Part b) (2017): Several RIA aiming at research and development of novel CBRN technologies and innovations identified in the above-mentioned catalogue will be selected by the European Commission. Each of these actions will be led by an SME. Each consortium implementing such a RIA must not only establish a consortium agreement among its members, but also a collaboration agreement with the participants in the CSA supported through Part a). Such a collaboration agreement must settle how the results from the RIA will be exploited and integrated into platforms managed by the CSA.

Expected impact:

- Shorter time to market for novel CBRN technologies and innovations, and more business deals leading to industrial products of interest to more practitioners in Europe (and world-wide).
- The larger the number of European companies involved in the CSA, the higher its impact will be.

General aspects of the topic

CSA (complementary grant) for (a) and RIA for (b)

Budgetary indication for proposers:

- In 2016, about 1.5 MEUR per action. No more than 1 action to be financed for this topic;
- In 2017, about 3.5 MEUR per action. No more than 4 actions to be financed for this topic.

DRAFT

TRL level: 4 to 8 for RIA

Conditions for the topic/eligibility criteria

The CSA must commit to issue: at months 3 and 9 each year, during at least three years of activities, the above-mentioned catalogue of technologies; at month 6 each year, the reports of their discussions; and at month 12 each year, the above-mentioned assessment of impact.

Each RIA must establish its « normal » consortium agreement, as well as a "Collaboration Agreement" with participant(s) in the CSA. A draft of the "Collaboration Agreement" must be attached to the RIA proposal, and endorsed by at least one participant in the CSA. The following options of the Model Grant Agreement will be implemented:

- 41.3 option 1 in RIA
- 41.4 option 1 in RIA and CSA
- 31.6 option 1 in RIA

All beneficiaries of the RIA grant agreements must be independent from each beneficiary in the CSA.

Each RIA proposals must be coordinated by an SME.

DRAFT

Sub Call – Fight against crime and Terrorism

The ambition of this sub-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.

DRAFT

SEC - FCT 1 - 2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection

Specific challenge:

Radicalisation leading to violent acts can have a huge impact on the society and its citizens: politically (seeding division between communities), economically, emotionally, and in terms of security. The roots of radicalisation are not well-known, whilst well-targeted response to emerging challenges of violent extremism cannot be developed without a full understanding of what drives the process of radicalisation and of how individuals may react to countermeasures. Also, terrorist groups and extremists are capitalising on advances in technology to spread propaganda and radical behaviours, but traditional law enforcement techniques are insufficient to deal with these new, evolving trends in radicalisation. The key in democratic societies is to ensure citizens' rights to free thought – even radical thought – while protecting society from the fallout of illegal actions from violent radicalised groups and individuals.

Scope:

Terrorism in Europe now finds its inspiration in a larger variety of ideologies, as described in the 2013 Europol TE-Sat report: nationalist, anarchist, separatist, violent left-wing or right-wing ideologies, or Al Qaida- or Daesh-inspired ideologies.

Preventing and countering radicalisation must engage the whole of society, and requires a holistic treatment, and a multidisciplinary approach.

Factors constituting a violent radicalisation process can be many: familial, social, socio-economical, psychological, religious, ideological, historical, cultural, political, propaganda-, social media- or internet-based. Events and conditions leading a person from ideas to violent action are also numerous, and mechanisms so complex that they need to be broken down to be understood.

Radicalised individuals, including recent converts, Europeans or foreigners, get organized in various ways: centralised and hierarchical organisations; networks; smaller groups based in Europe or on foreign territories; cells; and lone actors operating in a more unconstrained and unpredictable way. It is important to understand how networks and groups act towards the violent radicalisation of individuals.

Further to the recommendations of the Radicalisation Awareness Network, and to the work undertaken in the ongoing FP7 and other projects in the area, a better understanding of the causes and processes may lead to innovative, ethical solutions to counter violent actions taken by radicalized individuals (policies for preventing violent extremism; counter-communication disseminated either online (YouTube, special forums, Twitter etc.) or offline (in the classroom or in one-to-one interventions for example), since preventing violent radicalisation is also about winning the hearts and minds and countering extremist propaganda; surveillance, investigation, and protection techniques; forensic tools), whilst preserving the fundamentals rights of the citizens.

While Societal Challenge 6 mainly focuses on studying the phenomenon of radicalization, proposals under this topic should focus on developing policy recommendations and practical solutions to be implemented by security end-users.

Expected impact:

As a result of this action, security policy-makers and law enforcement agencies should benefit from a full set of policy recommendations and tools aimed at improving their ability to prevent and detect radicalisation by national and local security practitioners in a timely manner, i.e. before individuals turn towards violent, criminal or terrorists acts, including:

DRAFT

- Comparative analysis of different types of policies (e.g. preventive vs. legal and administrative measures) including counter-propaganda techniques;
- Improved description of competencies, skills and characteristics of the various types of practitioners involved in preventing, detecting or countering violent extremism;
- Improved information exchange between the different actors involved, including security practitioners, family of the radicalised individual, school/workplace of the radicalised individual;
- Field-validation of new approaches to anti-radicalisation directly applicable to support practitioners.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 3 MEUR per action. About 16 MEUR will be allocated to SEC – FCT – 1 and SEC – FCT – 2 altogether in 2016.

International cooperation: yes ☒ / no ☐

Possible classification: yes ☒ / no ☐

SSH-relevant: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no: Practitioners from various disciplines, including Law Enforcement Agencies from at least 5 EU Member States.

DRAFT

SEC - FCT 2 – 2016 – 2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts.

Specific challenge:

The European Union (EU) consists of more than 500 million people across the twenty-eight countries which make up the Union. Economic growth, together with the opportunities provided by a free and democratic society based on the rule of law, generate prosperity amongst Europe's citizens who benefit from increased mobility across national borders, and from globalized communication and finance infrastructure – but with such opportunities also come risks, as terrorists and criminals seek to pursue destructive and malicious ends. There are a number of significant common threats which have a cross-border impact on security and safety within the EU[4], and security has become a key factor in ensuring a high quality of life in the European society and in protecting our critical infrastructures through preventing and tackling common threats. The European Union must prevent, and if necessary investigate and mitigate the impact of criminal acts, whilst protecting fundamental rights of its citizens. The consistent efforts made by the EU Member States and the Union to that effect are not enough, especially when criminal groups and their activities expand far beyond national borders.

Scope:

The Lisbon Treaty enables the EU to act to develop Europe as an area of justice, freedom and security. Further to the Stockholm programme, an EU-wide approach to security, integrating prevention, investigation and mitigation capabilities in the area of fight against crime is increasingly required.

The definition of a European Security Model which builds upon the analysis of the human factors at the roots of the design of security strategies and methodologies, is needed. Such a Model would encompass: the development of a common understanding of security issues among EU security practitioners, as well as of the causes and effects of insecurity among EU citizens; common EU methodologies to be implemented by security practitioners (about enhancing prevention and anticipation and/or the timely involvement of all the actors that have a role in protection from the political, economic and social scene).

The globalization of communications and finance infrastructure allows for cybercrime to develop, and corruption and financial crime to take new forms. Cyber criminality is a phenomenon by which criminal acts with new tools and within a new environment, which is not satisfactorily understood, nor properly addressed. The same applies to the innovative technologies and methodologies for financial crime. Law Enforcement Agencies need new equipments to counter such developments.

In that context, proposals must fit under one of the following sub-topics:

Sub-topic 1. New methods for the protection of crowds during mass gatherings;
Sub-topic 2. New methods to prevent, investigate and mitigate cybercriminal behaviours;
Sub-topic 3. New methods to prevent, investigate and mitigate corruption and financial crime to fight the infiltration of organised crime in the European Union (licit) economy;
Sub-topic 4. New methods to prevent, investigate and mitigate high impact petty crimes;
Sub-topic 5. New methods to prevent, investigate and mitigate high impact domestic violence.

[4] Internal Security Strategy for the European Union: "Towards a European Security Model", Council of the European Union, 7120/10, to be followed by the new European Agenda for Security

Expected impact:

The EU law enforcement agencies will benefit from improving and consolidating knowledge about security problems and their remedies.
In detail, and for each sub-topic:

- A policy-making toolkit, for security policy-makers, to advance towards a European Security Model applicable by European law enforcement agencies and/or
- Common approaches to assessing risks/threats and identifying relevant risk-based security measures, including through acceptance tests (that take due account of legal and ethical rules of operation) and cost-benefit considerations and/or
- Better understanding of how the citizens perceive security and how it affects their feeling of insecurity, and in connection with potential limitations to, or risks of violations of privacy, and the consequent challenges for LEAs;
- Toolkits for law enforcement agencies, based and validated against the needs and requirements expressed by practitioners, and improving the perception by the citizens that Europe is an area of freedom, justice and security.

The societal dimension must be at the core of the activities proposed within this topic.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 3 MEUR per action. About 16 MEUR will be allocated to SEC – FCT – 1 and SEC – FCT – 2 altogether in 2016. No more than 2 actions to be financed for SEC – FCT – 2 in 2017.

International cooperation: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐ If yes how many?: Practitioners from various disciplines, including LEAs from at least 5 EU Member States or Associated Countries

Other specific eligibility criteria:

- For each Sub-topic, only the best proposal may be funded.
- Any proposal must include a workpackage for practical demonstrations.
- Only the sub-topics not covered in 2016 will remain eligible in 2017. A list of topics that remain eligible in 2017 will be published in due time.

DRAFT

SEC - FCT 3 - 2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA

Specific challenge:

Trace evidence are essential for law enforcement and justice. Forensic investigations of trace evidence contribute to the reconstruction of crimes. Answers to how and when a trace was deposited may already be of great help in the initial phase of investigation, provided that such answers become quickly available, and at an acceptable cost.

As for DNA trace, the additional challenge is to build up an image of an unknown perpetrator of a crime, drawing from as many traces and sources and as fast as possible (preferably directly at the crime site), within legal and ethical constraints.

Scope:

The forensic community still requires:

a) Furthermore, in the specific area of trace qualification:

- Better knowledge of the composition of traces; of the time when they were left, whether they result from crime-related or inoffensive activities; of the effect, on the quality of traces, of the time elapsed between the moments when there are deposited and collected; of the transfer mechanisms, persistence and recovery of traces; of the circumstances of the trace deposit;

- New tools, to be used in the field, that can detect, collect and analyse traces, and assist in the interpretation of trace data with a view to avoiding practitioner's biases;

b) Alternatively, in the specific area of DNA extended exploitation:

- Tools and techniques, and advanced methods for data analysis and statistical interpretation to extend the exploitation of DNA, which implement "privacy by design" (that take account of the status of personal data depending on the EU Member State legislations.

- New method for complete sequencing to establish genetic composite sketch.

In addition, regarding both a) and b), proposals need: to address the issue of admissibility of evidence once securely transmitted to and from forensic experts in the field or in laboratories; to propose curricula for the training forensic investigators to use these new tools, techniques and methods; to propose methodologies to compare results produced by forensic organizations across Europe to contribute to the EU-wide consistency of forensic work.

Expected impact:

All proposals should contribute to:

- Solving crimes more rapidly to reduce societal distress, investigative costs and the impact on victims and their relatives;
- Improving forensic capabilities to evaluate different hypotheses used in criminal investigation and prosecution;
- Providing forensic experts with instruments to avoid unnecessary analysis costs and time spent by forensic labs, and thus render the forensic process more efficient;
- Preventing miscarriage of justice due to the misinterpretation of forensic findings by the courts.

In addition:

- Those proposals addressing a) should contribute to the better identification and understanding of crime related traces and the activities that have led to the deposition of the traces;
- Those proposals addressing b) should contribute to the enhancement of the ability to obtain reliable information from DNA samples.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 5 MEUR per action. About 26 MEUR will be allocated to SEC – FCT – 3, SEC – FCT – 6 and SEC – FCT – 7 altogether in 2016.

Maximum two project to be financed for this topic?: yes ☒ / no ☐ One addressing the general issues and a), and one addressing the general issues and b).

International cooperation: yes ☒ / no ☐

TRL level: **5**

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: Forensic laboratories or institutes from a minimum of 5 EU Member States

DRAFT

SEC - FCT 4 - 2017: PCP of toolkits integrating tools and techniques for forensic laboratories

Specific challenge:

Since 2011 the EU has developed a vision about European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe.[5]

A wide, heterogeneous, variety of forensic tools are in use or being developed across Europe, making the comparison and exchange of information among forensic laboratories difficult and sometimes impossible, which limits the use of forensic data in cross-border investigations, and in foreign courts. Forensic data need to be quickly available, at an acceptable cost, across borders.

Scope:

The most promising forensic techniques need to be developed further, and brought up from experiment to a toolkit usable on a daily basis across Europe. This can be achieved if forensic laboratories from a broad variety of EU countries with diverse legal systems agree on common standards and join forces along the following steps:

Phase 0: To prepare an inventory of forensic technologies already available at TRL 4 or 5, and to identify, within all areas covered by the various ENFSI working groups (http://www.enfsi.eu/), a subset of technologies to be brought at TRL 8;

Phase 1: To prepare the tenders packages for calls for tenders to build prototypes of a toolkit integrating the above-mentioned subset of technologies, that can be used across Europe; To develop EU-wide benchmarks and validation methods for forensic technologies;

Phase 2: To implement the calls for tenders to generate 2 prototype toolkits from 2 different sources;

Phase 3: To benchmark and validate the 2 toolkits against the methods developed during Phase 1;

Phase 4: To draft a curriculum for pan European training in forensic technologies, and to plan for its assessment across Europe; to initiate the EU-wide certification of the toolkits based on the results of Phase 3.

Expected impact:

- Advanced forensic toolkits usable across the EU an providing comparable results admissible in court;
- Path towards an EU-wide certification mechanism.

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: about 10 MEUR per action. No more than one action to be financed for this topic

[5] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/126875.pdf

DRAFT

Possible classification: yes ☐ / no ☒

TRL level: **8**

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: Forensic laboratories or institutes from a minimum of 5 EU Member States or international organisations

Other specific eligibility criteria:

To ensure that the outcome of the PCP action becomes also available to non-participating Member State organisations for further capability or product procurement purposes, the proposals must necessarily state the:

1. Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product fully or partly derived from the PCP action the use of the information required to run such a procurement process, and solely for that purpose.
2. Commitment from participating procurement authorities to involve the PCP beneficiaries in the decision on which information to release, for the purpose set out in paragraph 1.
3. Commitment from participating procurement authorities to negotiate the use granted under paragraph 1 on fair, reasonable and non-discriminatory (FRAND) terms.

DRAFT

SEC - FCT 5 - 2017: Integration of detection capabilities and data fusion with utility providers' networks

Specific challenge: Research undertaken in recent years has proposed innovative approaches for the detection of precursors of explosives, drugs, and more generally speaking substances threatening the security of the citizens. Such approaches often require the installation of networks of sensors throughout urban areas. Utility networks, which are well developed in such areas, could be both sources of information through the analysis of the substance that they transport/provide (e.g. energy consumption, characteristics of used waters) or of their environment (e.g. quality of air, etc.). They can constitute networked (mobile) platforms for sensors, but this potential remains largely untapped.

Scope:

Proposals should address the deployment of detection systems in large and medium cities, in existing networks, or a combination of such networks, for instance for the detection of explosive precursors and illegal chemicals (drugs). Proposals shall address sewage networks and quality of air monitoring networks, and may address other networks. The experiment should last a significant period of time (at least two years).

Proposals should also provide for a mobile platform equipped to ascertain the composition and location of suspicious measurements, once data have been provided by the networked detection systems.

Proposals should provide for the prototype of a system controlling the detection systems and capable of fusing data provided by a variety of such networks, and of interfacing with other networks, pay particular attention to ethical issues raised when using such systems, and address the sustainability of such systems.

Expected impact:

- Real-life demonstrations of the combination of systems detecting precursors of explosives, and drugs, installed on at least two utility networks, and making use of a prototype of information systems fusing the data provided by these networks;
- Better understanding of the effectiveness of the combination of technologies used to detect and locate a bomb factory or a drug lab/drug consumption/traffic;
- Provision of a higher level of information/intelligence to those involved in counter-terrorist and countering drugs activities (e.g. Law Enforcement Agencies, Security & Intelligence Agencies, and Government Laboratories)

General aspects of the topic

Innovation action

Budgetary indication for proposers: about 8 MEUR per action. No more than 2 actions to be financed for this topic

Possible classification: yes ☒ / no ☐

SME relevant: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: 7 to 8 for the sensors deployed; 6 for the control and information system, and the mobile platform.

Conditions for the topic/eligibility criteria

DRAFT

Practitioner participation mandatory?: yes ☒ / no☐: At least two independent utility network operators; and LEA in charge of counter-terrorism, or bomb squad units, from at least 3 EU Members States.

Other specific eligibility criteria:

Demonstrations must take place in at least 2 agglomerations: One of over 1,000,000 inhabitants, and another of between 100,000 and 300,000 inhabitants, located in 2 different Member States, and using different types of sewage systems (separating domestic waters from rain waters, or not.).

DRAFT

SEC - FCT 6 - 2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot

Specific challenge: Extensive research has developed, in recent years, methods and techniques to enhance support to those involved in countering explosive threats, including efforts to counter Improvised Explosive Devices (IED) and Home-Made Explosives (HMEs). But up until now, no comprehensive research has assessed the effectiveness, the efficiency and the cost of the combination of these methods and techniques (including those developed outside of these civilian sphere) to stop the threat at some point in time before the attack.

Scope:
Innovative approaches are required to: assess the effectiveness of the methods and techniques used to counter a threat at certain point in time of the plot, against a credible scenarios based on real cases; assess how to best combine methods and techniques along the timeline of a plot; identify methods and techniques able to fill in existing gaps.
Methods and techniques to be considered include:
- Intelligence to spot those preparing for an attack;
- The inhibition of precursors;
- Detection of specific chemicals, bomb factories, and/or IED;
- Neutralization of IED;
- Identification of weakness of the current defences against IED, and possible improvements.

No technological development is foreseen, but rather operational research building upon the work of the European Network of Detection of Explosives (NDE). The results of the action should serve as a basis for the future development of new and innovative detection techniques on explosives to create a step change from current methods and technologies.

Expected impact:
- Better knowledge of the effectiveness of the supporting methods and techniques and of the combination of technologies used to detect and locate an explosive and to counter the terrorist use of an explosive threat.
- Better understanding of the weakness of current defences againts IED.
- Stronger involvement of practitioners in the field of counter-terrorist activities (e.g. Law Enforcement Agencies, bomb disposal units, Security & Intelligence Agencies, and Government Laboratories) in making assessing and selecting new tools and technologies.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 5 MEUR per action. About 26 MEUR will be allocated to SEC – FCT – 3, SEC – FCT – 6 and SEC – FCT – 7 altogether in 2016. No more than 1 action to be financed for this topic.

Possible classification: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: Practitioners in the field of counter-terrorist activities from at least 3 EU Member States or Associated Countries.

DRAFT

SEC - FCT 7- 2016 - 2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism.

Specific challenge:

Organized crime is often at the forefront of technological innovation in planning, executing and concealing their criminal activities and the revenues stemming from them. Law Enforcement Agencies are often lagging behind when tackling criminal activities supported by "advanced" technologies.

Scope:

- New knowledge and targeted technologies for fighting both old and new forms of crime supported by advanced technologies;
- Test and Demonstration of newly developed technology by LEAs involved in proposals;
- Innovative curricula, training and (joint) exercises to be used to facilitate the EU-wide take-up of these new technologies, in particular in the fields of:

  Sub-topic: 1. cyber-crime: virtual/crypto currencies des-anonymisation/tracing/impairing where they support underground markets in the darknet (e.g. Deep Web)
  Sub-topic: 2. detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas, and involving as beneficiaries, where appropriate, the operators of infrastructure
  Sub-topic: 3. video analysis in the context of legal investigation
  Sub-topic: Others.

Proposals in additional areas (Sub-topic: "Others") are welcome, provided that it involves a sufficient number of LEAs (see eligibility criteria).

Expected impact:

- Crimes solved more rapidly, to reduce societal distress, investigative costs and the impact on victims and their relatives;
- Improved investigation capabilities;
- LEA officers provided with better tools to help them on their (specialized) daily work;
- Better identification and understanding of criminal activities

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 5 MEUR per action. About 26 MEUR will be allocated to SEC – FCT – 3, SEC – FCT – 6 and SEC – FCT – 7 altogether in 2016. No more than 2 actions to be financed for SEC – FCT – 7 in 2017.

TRL level: **6**

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐:

- In Sub-topic: 1, Sub-topic: 2 or Sub-topic: 3: a minimum of 3 LEA from 3 EU Member States

DRAFT

- In other fields (Sub-topic: "Others"): a minimum of 5 LEA from 5 EU Member States or Associated Countries

Other specific eligibility criteria:

- For each Sub-topic, only the best proposal may be funded.
- Proposals on detection technologies are excluded from this topic.
- Any proposal must include a workpackage for field demonstrations.
- Only the sub-topics not covered in 2016 will remain eligible in 2017. A list of topics that remain eligible in 2017 will be published in due time.

DRAFT

Sub Call – Border Security and External Security

On the one hand this sub-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, contributing to the further development of the European Border Surveillance System (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 sub-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.

DRAFT

SEC – BES 1 – 2017: PCP of next generation of information systems to support EU external policies

Specific challenge:

The broad range and the complexity of Common Security and Defence Policy civilians' missions make the management of information and of resources critical to decision-making, planning, optimizing for pre-deployment, and deploying capabilities within such missions, and essential to increase the efficiency, visibility and impact of the missions.

The processes, procedures, information systems, and equipment currently committed to such missions by the Member States need to be brought together and coordinated to constitute a common interoperable platform to enhance the EU capacity to play its role.

Scope:

This topic is to support the development of a cost-effective common Situational Awareness, Information Exchange and Operation Control Platform.

Cost-effectiveness, and shorter time to implement may result from adapting and exploiting existing approaches and experience in the defence sector, and leveraging from results from relevant projects formerly funded by the EU.

Taking into consideration the findings of the CSA under topic "BES-11-2015: Information management topic 2: Information management, systems and infrastructure for civilian EU External Actions" of the 2014-2015 Secure Societies Work Programme, activities must be structured along the following phases:

Phase 1: Based on common performance levels, requirements and associated specifications for the development of a cost-effective common situational awareness, information exchange and operation control platform for EU civilian external actions developed in BES-11-2015, to be published prior to the opening of the Call, plan the research and the design of the platform.

Plans must consider integrating existing technologies and methodologies (including pooling and sharing of capabilities) according to design constraints expressed by the buyers, to ensure cost effectiveness and interoperability.

The results of phase 1 should lead to calls for tenders (for the procurement of R&D services) which focus on technologies clearly identified to be part of a unique architecture.

Phase 2: The research and specification work should lead to at least 2 flexible platforms to support, each, several scenarios for EU actions under different framework conditions.

Phase 3: By the end of 2020, the project should have documented, tested, and validated the use of each platform in at least two operational scenarios within actual multinational operations. The participation of relevant and competent authorities in the consortium of buyers is a prerequisite.

Expected impact:

- At least two prototype platforms deployed and tested in several, different real-life environments.
- Better integration of existing systems and methodologies in situational awareness, information exchange and operation control platform prototypes.
- Solid basis for a full-scale, cost-effective common situational awareness, information exchange and operation control platform for EU civilian external actions.

DRAFT

- Improved management of EU resources' allocated to EU civilian external actions.

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: about 10 MEUR per action. No more than one action to be financed for this topic

Possible classification: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: 8

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: a minimum of three potential users/buyers of such systems from three different EU Member States

Other specific eligibility criteria:

To ensure that the outcome of the PCP action becomes also available to non-participating Member State organisations for further capability or product procurement purposes, the proposals must necessarily state the:

1. Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product fully or partly derived from the PCP action the use of the information required to run such a procurement process, and solely for that purpose.
2. Commitment from participating procurement authorities to involve the PCP beneficiaries in the decision on which information to release, for the purpose set out in paragraph 1.
3. Commitment from participating procurement authorities to negotiate the use granted under paragraph 1 on fair, reasonable and non-discriminatory (FRAND) terms.

DRAFT

SEC - BES 2 – 2016: Towards reducing the cost of technologies in land border security applications

Specific challenge:

Border management in European Union context means first and foremost the enforcement of the common policies and implementation of the common rules. As international travel flows continue to rise, there is growing pressure to process large volumes of people at border crossing points without delays. At the same time, the smuggling of people across the borders is growing. However, the external land borders of the European Union (and border crossing points) present a wide range of challenges, ranging from those relevant to Nordic Countries, to those of Greece.

The European Border Surveillance System (EUROSUR) is establishing a mechanism for Member States' authorities carrying out activities at the European Union external border to share operational and situational information and pictures. But without investments in technology and information systems, it is simply not feasible to manage borders and border crossing points. Whilst technology offers great potential to meet the dual objective of enhancing border security while facilitating cross-border travel, its costs are often prohibitive, especially in the light of the current national budgets. Furthermore, the broad variety of heterogeneous IT applications and systems deployed for land border security makes their management increasingly complex and costly. Innovative, cost-efficient technologies are needed, or existing ones need to become more affordable, to meet border authorities and practitioners' requirements, and budgetary constraints.

Scope:

The cost of a broad variety of technologies could be made more affordable, in priority those used at border crossing points bearing the heaviest burden (based on the analysis of flows of people and of smuggling methods, associated risks, and bottlenecks in surveillance and/or control.)

The relevant border authorities are in the best position to identify the most relevant portions of the EU land borders that could benefit from more cost-effective solutions.

Cost reduction may result from: merging several advanced technologies into novel border security solutions; trade-off against performance; optimizing the use of technologies where they are most effective at mitigating risks further to specific risk analysis; achieving greater interoperability among systems; enabling the early provision of data in advance to the time of crossing.

The availability or scarcity of human resources and of space, the need for portable and versatile solutions are other parameters to be taken into account when considering the added value and cost of novel technologies solutions, including in terms of societal and ethical value and cost. In particular, the design of more homogeneous IT platforms, sharing an interface common to all operational databases and border security applications, is desirable to make their management less ressource intensive.

Overlap with the work being undertaken by border surveillance authorities in the context of the EWISA project should be avoided, whilst compatibility with previous results from FP7 or H2020 projects is encouraged.

Expected impact:

- Novel technologies, tools and systems (higher TRLs) demonstrating very substantial cost-reduction compared to existing technologies, tools and systems.

DRAFT

- Cost-reduction shall be assessed through the comparative testing of technologies, tools and systems in quasi-operational scenarios. Cost vs. benefit analysis must take account of functional needs, conditions of use, maintenance costs, performance and quality, impact on operating procedures, impact on travellers, training requirements for new skills, etc.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 5 MEUR per action. No more than 2 actions to be financed for this topic

Possible classification: yes ☒ / no ☐

SME relevant: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **6**

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard authorities from 3 different EU or Schengen Member States

DRAFT

SEC - BES 3 – 2017: Risk-based screening at border crossing

Specific challenge:

The concept of 'borders' has changed in recent times. The purpose and function of borders have been, and remain, to delineate and demarcate one sovereignty from another. However, borders must also allow for the smooth movement of people and goods.

Maintaining the current level of checks is becoming increasingly expensive given the ever growing volumes of people and goods on the move, and increasingly more disruptive of flows. It would remain sustainable if thorough checks could be limited to fewer individual goods and people pre-selected further to a preliminary (and non-disruptive) risk-based screening of the flows.

Scope:

Proposals should take account of the four-tier access control model developed in the EU: measures undertaken in, or jointly with third countries or service providers (e.g. those managing Advance Passenger Information or Passenger Name Record systems); cooperation with neighbouring countries; border control and counter-smuggling measures; control measures within the area of free movement in order to prevent illegal immigration and cross-border crime inside the Schengen area.
Innovative, international alert systems can be developed further to more co-operative law enforcement and investigative efforts. Building upon lessons learned and field experience is essential.
The combination of a variety of arrays of sensors, new operational methods, and improved data management techniques can support appropriate law enforcement responses and enable better, transnational, interagency access to reliable and secure situational intelligence and information, on a real-time and cost-effective basis.
Collaboration with IATA, the air transport industry and other partners and international stakeholders in other fields of transport safety (e.g. maritime, rail) may lead to the development of new solutions.
Particular attention should be paid to personal data protection and to other ethical concerns that may arise from the development of risk-based screening at borders.

Expected impact:

- More effective use of intelligence to reduce risks at borders;
- Enhanced situational awareness for border control practitioners, enabling the timely and proper identification of potentially dangerous people and goods, and preventing smuggling and human trafficking;
- Improved risk-management coordination and cooperation between border control (passport/persons), customs (baggage/goods) and security in transport (pre-boarding security checks on persons and baggage);
- Improved solutions for remote detection of abnormal behaviours;
- Improved and people-respectful border automated screening systems through close cooperation with actiosn resulting from SEC-BES-6.

General aspects of the topic

Innovation Action

Budgetary indication for proposers: about 8 MEUR per action. About 18 MEUR will be allocated to SEC – BES – 3 and SEC – BES – 5 altogether.

Possible classification: yes ☒ / no ☐

TRL level: 7

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard authorities from 3 EU or Schengen Member States

DRAFT

SEC - BES 4 – 2017: Through-foliage detection, including in the outermost regions of the EU

Specific challenge:

Member States' authorities are carrying out activities all along the European border, and have started to share operational and situational information. But several regions at the borders of the European Union are covered with forests, and face extreme temperature conditions. Detecting, locating, tracking or identifying persons and vehicles crossing the border in forested regions is extremely difficult given that technologies for surveillance through harsh unstructured environments are currently not effective. The increasing risk of irregular flows and immigration across the border with, for instance, Turkey, Ukraine, Belarus, Russia or Brazil makes the issue even more acute than in the past.

Scope:

Systems should be developed that combine or improve surveillance technologies and techniques and arrays of sensors of different sorts capable to provide higher quality detection capabilities and imaging via the integration of different techniques, to achieve wide- and small-area through foliage detection, despite the canopy density, in a real operational context. They could build on airborne, satellite-based, and/or on ground based platforms.

Solutions should be tested and validated in terms of capabilities to control effectively the land border covered by a vegetation layer, in all weather conditions.

Pre-competitive research may be needed to address various stages of development, from sensor design, to the analysis and design of system configuration and to the integration and validation by (public) authorities for target detection, identification and recognition.

Overlap with the work being undertaken by border surveillance authorities in the context of the EWISA project should be avoided, whilst compatibility with previous results from FP7 or H2020 projects is encouraged. Ethical and societal acceptance needs to be properly addressed.

Expected impact:

- Improved border surveillance and search-and-rescue capabilities, especially in forested regions;
- Validated through-foliage detection technologies, in terms of fitness for purpose, low rate of false alarms, practicability, mobility, and cost effectiveness.
- Demonstrated through-foliage detection technologies in the context of realistic operational scenarios, in extreme weather conditions, to be implemented in collaboration with the relevant border surveillance authorities and in regions where the Frontex Agency indicates that important illegal border crossing and smuggling may be taking place.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 8 MEUR per action. No more than one action to be financed for this topic

Possible classification: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **5 or 6**

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard authorities from 3 EU Member States

DRAFT

SEC - BES 5 – 2017: Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements

Specific challenge:

Effective management of risks in the international supply chain is crucial to ensuring the security (and safety) of EU residents, the protection of the financial and economic interests of the EU, while at the same time facilitating legitimate trade. The "*EU Strategy and Action Plan for customs risk mana*gement" (COM (2014) 527 final) Communication of the Commission drafts a strategy and an action plan for improving customs risk management and supply chain security. It identifies the need for customs and other competent authorities to acquire quality data on supply chain movements, to exploit them for risk assessment purposes, and to consequently adapt organizations and strategies for checks to make more efficient.

Scope:

Risk management of the movement of goods through the international supply chain requires identifying, evaluating and analysing the full range of largely diverse threats and risks associated with goods and their movements, at the EU, national, and intercontinental levels. It starts with the identification, by the custom authorities themselves, of the most serious risks, so that necessary controls are carried out at the most appropriate time and place.

Strategies and tools are needed for the timely submission to customs authorities of relevant high-quality and comprehensive data on goods moving and crossing borders, whilst taking into consideration the national and EU legal, procedural and IT systems where they exist. Realistic methodologies and organisations need to develop, that facilitate collaboration among the relevant authorities (not only customs but also law enforcement, security and border control agencies). Data governance policies and mechanisms for data sharing need to be agreed internationally.

Common repositories that take advantage of existing instruments such as the Advance Cargo Information System (advance electronic notification of cargo coming into EU before it leaves the third country) which are under-utilised and under-exploited for risk management purpose, can support the intelligent use and management of complex and large amount of data, exploiting unstructured data, supporting operational and situational awareness of customs authorities, adding intelligence (trends analysis, correlation analysis, etc.) by means of state-of-the-art technologies including in the fields of Big Data, Data Analytics, Data mining, Visualization, Intelligent User's Interfaces, Insight knowledge and knowledge representation, artificial intelligence, automatic language translation. The governance of access to such repositories need to be addressed.

Expected impact:

- Contribution to the implementation of the EU strategy and action plan for customs Risk management (COM (2014)527) endorsed by the Council in December 2014, and an integral part of the European Agenda for Security.

- Proposals for making better use of additional Advance Cargo Information (ACI) – currently being discussed as part of a supplementary Delegated Regulation to EU Reg 952/2013 (in relation to the Union Customs Code);

- Reduction of terrorist threats; illicit trading of arms; illicit trading, in general, and counterfeiting; drug trafficking; illegal border crossing; trafficking in human beings; smuggling;

- Mitigation of risks resulting from capacity shortages in some Member States, by addressing risks in a transnational manner;

DRAFT

- More effective and efficient information sharing among customs within Europe, as well as between customs, security and law enforcement agencies within individual countries, with a view to improving checks at the external border of the relevant European areas;

- Cost-effective solutions to complement national action;

- Specifications of a common external interface supporting a commonly agreed access governance.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 5 MEUR per action. About 18 MEUR will be allocated to SEC – BES – 3 and SEC – BES – 5 altogether.

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard or custom authorities from 3 EU or Schengen Member States

DRAFT

SEC - BES 6 – 2017: Acceptance of "no gate crossing point solution"

Specific challenge:

For the traveller it would be ideal to cross borders without being slowed down. It is indeed likely that, in the next 10 years or so, technologies make it possible to implement "*no gate crossing point solutions*" that allow for seamless crossing of borders and security checks for the vast majority of travellers who meet the conditions of entry, and make sure that those who do not fulfil such conditions are refused entry.

There is a broad variety of technologies and systems including information systems and (networks of) sensors that will become available to support border checks based on risk-assessment methods. Some are to be deployed in the vicinity of border crossing points, others can be mobile and used to check travellers data along his/her journey.

However, in the intensive use of technologies that this will require bears the risk to invading people's privacy, and the societal and political acceptance of technologies for "no gate solutions" is required prior to their implementation.

Scope:

The assessment of the acceptability of such (combinations of) technologies and systems by citizens (who need to remain in control of personal data) and practitioners is needed, that takes account of human behaviour, legal frameworks, societal issues, and possible risk of discrimination.

Methods developed to perform such assessments need also to generate information useful for decision makers to take informed decisions about future technology deployments, and for industry to design products that preserve privacy.

Expected impact:

- Information systems that better manage personal information and support the automated checking and analysing of various entry and exit data, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-BES-3.
- Networks of sensors that better collect information needed for border checks, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-BES-3
- A method, and metrics, to assess acceptability by the society of the concept of border control processes based on "no gate crossing point solutions", and of the various technology components that may be required.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: about 3 MEUR per action. No more than two actions to be financed for this topic.

Possible classification: yes ☒ / no ☐

SSH-relevant: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

DRAFT

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard authorities from 3 EU or Schengen Member States

DRAFT

SEC - BES 7 - 2016: Data fusion for maritime security applications

Specific challenge:

In coherence with the objectives of regulation No 1052/2013 establishing the European Border Surveillance System (EUROSUR), the Action Plan for the EU Maritime Security Strategy (EUMSS) advocates the "*strengthening of [...] the information exchange to optimise the surveillance of the EU maritime area and its maritime borders*" and "*the improvement of the situational awareness and increase reaction capability at the external borders of the Member States of the Union for the purpose of detecting, preventing and combating illegal immigration and cross-border crime, and contributing to ensuring the protection and saving of lives of migrants*").

Large amounts of "raw" data are being collected nowadays, at unprecedented scale, coming from different sources, from different sorts of assets from different EU Member States, from the Internet and social networks, and gathered for different security purposes, in a variety of formats, are available but not necessarily exploitable because they are not accessible at the same time nor interoperable, until they are "fused" and made "understandable" to all systems supporting information exchange, situational awareness, and decision-making and reaction capability at the EU external maritime borders.

Scope:

Many detection systems are available to collect data that are useful for maritime security, coastal surveillance and beyond. The fusion of these data requires the development of methods and tools that take account of the technical characteristics of existing systems, and the specific context of all aspects of maritime security.

"Fusion" may refer to *"intelligence correlation to produce higher level (or more accurate) information*". It may involve, inter alia:

- mixing several homogeneous data to produce another data of superior quality;
- pre-processing raw data and associating heterogeneous data, produced by different types of sensors, that refer to the same actual object or event, to produce information of superior quality;
- overlapping surveillance pictures produced by different sources and generate a picture without redundant objects/tracks and allowing to deal with faulty sensors and data;
- combining data acquired at different points in time through sensors (e.g. radars and camera) installed on the same platform or on different ones (underwater or surface vessels, drones or aircraft, satellite systems (including but not exclusively Copernicus, Galileo, and EGNOS);
- combining offline with realtime data.

Data fusion techniques, complementing the existing information systems and sensor platforms, should help focusing the geographical zones to monitor through the deployment of surveillance capabilities.

EU-funded R&D cooperative projects (such as PERSEUS, CLOSEYE, I2C and EU CISE 2020) and EU Agencies (e.g. the EDA with the IN4STARS project) have touched upon the issue.

Data fusion may bear on, or generate information needing classification. Ethical and societal issues need to be properly addressed.

Expected impact:

- Description of how to integrate the knowledge on data fusion originating from pre-existing EU-funded R&D cooperative projects;
- Contribution to the further development of EUROSUR and to the implementation of the EUMSS action plan;

- Improved and extended maritime border situational awareness;
- Improved operational support to search-and-rescue activities;
- Improved border surveillance systems in terms of information exchange, situational awareness, and decision-making and reaction capabilities;
- Solutions better fitting the existing systems and the actual concepts of operations set for missions involving the assets of several Member States maritime border surveillance, security and search-and-rescue organisations;
- Pre-standards to be followed by standardization procedures with the ESO;
- Solutions demonstrated in the context of interagency and cross-border cooperation;
- Solutions interfaced with existing infrastructure (systems, platforms and networks of sensors.).

General aspects of the topic

Innovation Action

Budgetary indication for proposers: about 8 MEUR per action. About 24 MEUR will be allocated to SEC – BES – 7 and SEC – BES – 8 altogether

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐ (participation of neighbouring countries is encouraged)

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **7**

Practitioner participation mandatory?: yes ☒ / no☐: At least 3 border guard authorities from 3 EU member states

Other specific eligibility criteria: Participation from at least 3 independent industry organizations established in 3 different EU Member States or Associated countries is mandatory.

DRAFT

SEC - BES 8 – 2016: Autonomous surveillance with enhanced command and control systems for the surveillance of borders in a 3D environment

Specific challenge:

Low levels of situational awareness on the EU borders, high at sea and on unpopulated or scarcely populated land areas, are important factors of cost of border surveillance. This could improve if the different prototypes of unmanned vehicles tested today to perform automatically a very limited set of functions and routines could be transformed into autonomous, long-endurant agents able to operate in complex maritime and land environments.

Current border control systems involve a wide range of heterogeneous assets – manned and unmanned – to survey from air, surface (land and sea) and underwater. Similarly the objects of their surveillance may be vessels, land vehicles, aircrafts, and underwater vehicles used, for instance, for smuggling and trafficking. Only enhanced command and control systems using advanced 3D computer graphics technology may allow to represent accurately the position of surveillance assets – including autonomous agents – and extrernal objects in such complex environments.

Scope:

The proposed action should cover one of the following sub-topics:

Sub-topic: 1. Autonomous surveillance

Autonomous agents should be adaptable: in order to deal, where applicable, with extreme and diverse weather and sea condition, including in the Artic region; interconnected: interoperable and capable of exchanging information among themselves and with the system's ground segment; tele-operable from the ground.

They should support missions ranging from surveillance to detection of marine pollution incidents, and including early identification and tracking of illegal activities and illegal communication.

They should operate as single units, but also in homogeneous or heterogeneous groups i.e. mixing aerial vehicles with fix, rotary wings (or tilt-rotor), unmanned surface vehicles (USV), unmanned under-surface vehicles (UUSV), unmanned ground vehicles (UGV) with different types of sensor and communication suites on board, customized according to operational and environmental needs and addressing cross-cueing.

Autonomous agents should exchange information at tactical level and interface with each others and with command and control systems as they exist, today, at different levels.

Sub-topic: 2. Enhanced command and control systems for the surveillance of borders in a 3D environment Autonomous surveillance

Enhanced command and control systems should integrate:

- air surveillance technologies (including radar technologies for the detection of low flying aircrafts);
- coastal and underwater surveillance technologies (including coastal radar, maritime patrol aircraft (MPA), light patrol aircrafts, unmanned aerial vehicles (UAV), Patrol Vessels, UUV, etc.);
- ground surveillance technologies (including UGV);
- satellite-based services;
- maritime information services;
- 3D cartography and bathymetry servers;
- 3D modelling of situational picture based on 3D computers graphics engines;

DRAFT

- augmented reality technologies;
- mobile devices and handsets such as tablets and smartphones.

Expected impact:

- The further development of the Common Information Sharing Environment (CISE) and of the European Border Surveillance System (EUROSUR);
- New technologies for autonomous surveillance systems;
- Improved, cost-effective and efficient unmanned platforms for border surveillance systems, and the detection of marine pollution incidents;
- Adaptation of long-tested technologies to the specific requirements of borders control area;
- Agents and command and control systems interoperable with existing, multi-country European infrastructure.

General aspects of the topic

Type of action: Innovation Action

Budgetary indication for proposal: about 8 MEUR per action. About 24 MEUR will be allocated to SEC – BES – 7 and SEC – BES – 8 altogether

International cooperation: yes ☒ / no ☐

Possible classification: yes ☒ / no ☐

TRL level: TRL 6 or 7

Conditions for the topic/eligibility criteria

SME participation mandatory: yes ☒ / no ☐

Practitioner participation mandatory?: yes ☒ / no: Practitioners from various disciplines, including Border guard authorities from at least 5 EU or Schengen Member States.

DRAFT

Sub Call - General Matters

DRAFT

SEC – GM 1 – 2016 and 2017: Pan European Networks of practitioners and other actors in the field of security

Specific challenge:

In Europe, practitioners interested in the uptake of security research and innovation (e.g. firefighters, police and intelligence communities, border guards, custom authorities, explosive specialists, forensic laboratories, medical emergency teams, etc.) are dedicated to performing their duty and to focusing on their operation. In general, practitioners' organisations have little means to free workforces from daily operations, and to dedicate time and resources to monitor innovation and research that could be useful to them. They have little opportunities to interact with academia or with industry on such issues. All stakeholders – public services, industry, academia – including those who participate in the Security Advisory Group, recognize it as an issue.

Scope:

Practitioners are invited to associate in 3 different categories of networks:

a) Practitioners (end-users) **in the same discipline and from across Europe** (some examples: firefighters; police and intelligence bodies; border guards, coast guards, and custom authorities; explosive specialists; forensic laboratories; medical emergency teams; think-tanks on security; etc.) can get together to: 1) monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results, 2) express common requirements as regards innovations that could fill in capability and other gaps and improve their performance in the future, and 3) indicate priorities as regards domains requiring more standardization;

b) Practitioners (end-users) **from different disciplines** and concerned with current or future security or disaster risk and crisis management issues **in a particular geographical area** can get together to: 1) monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results, 2) express common requirements as regards innovations that could fill in capability and other gaps and improve their performance in the future, and 3) indicate priorities as regards common capabilities, or interfaces among capabilities, requiring more standardization.

   Geographical priorities include:

   - the Mediterranean region (including the Black Sea): to enable an EU joint network concept for border protection and other security-related tasks, so that the entities in the network share information, collaborate better, and establish joint border surveillance scenario. The network should provide with human infrastructure organizing operations more efficiently and enable the coordinated use of interconnected information systems and national infrastructure in the whole region;
   - the Artic and North Atlantic region: to prepare to cope as a network with the security threats that will result from the opening of the Northern passages, which are very important for the development of the region, but from which seaborne disasters are likely to arise. The current lack of infrastructure makes dealing with catastrophic incidents quite a challenge. The region needs to prepare, taking into account geographical specificities (climate-related, demographic, topologic, and in relation with the functioning of space-based systems;)
   - the Danube river basin: to enable an EU joint network concept for disaster resilience, so that the countries of the region, which faces natural disasters, particularly flooding in a repetitive manner, can benefit at most from the EU civil protection mechanism;
   - the Baltic region: to enable innovative border control cooperation e.g. with respect to smuggling and other security related issues, to the trafficking in human beings, to maritime surveillance, and to macro-regional risk scenarios and gaps identification; to support the Baltic Sea Maritime Functionalities flagship initiative.

c) Entities from **around Europe** that manage **demonstration and testing sites, training facilities,** including simulators or serious gaming platforms in the area of CBRN and for first responders or civil protection practitioners, can get together to: 1) establish and maintain a roster of capabilities

DRAFT

and facilities, and 2) organize to share expertise, and 3) plan to pool and share resources with a view to optimize investments.

Opinions expressed and reported by the networks of practitioners should be checked against what can be reasonably expected, and according to which timetable, from providers of innovative solutions.

d) In addition, support will be given in 2017 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. The network should focus on issues specific to the "Secure societies …" challenge.

Expected impact:

- Common understanding of innovation potential, more widely accepted understanding, expression of common innovation and standardization needs among practitioners in the same discipline.
- More articulated and coordinated uptake of innovative solutions among practitioners from different disciplines who are often called to act together to face major crisis.
- More efficient use of investments made across Europe in demonstration, testing, and training facilities for first responders.
- Synergies with already established networks of practitioners, even if these networks are for the time being only dedicated to aspects of practitioners' work unrelated to research and innovation (in general, to the coordination of their operations).
- An improved and professionalised NCP service, consistent across Europe, thereby helping simplify access to Horizon 2020 calls, lowering the entry barriers for newcomers, and raising the average quality of proposals submitted.

General aspects of the topic

Coordination and Support Action

SME relevant: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

International participation from neighbouring countries is highly recommended for Part b)

Budgetary indication for proposers: about 3.5 MEUR per action for a duration of 6 years (recommended duration) for Parts a), b) and c); about 2 MEUR per action for a duration of 3 years (recommended duration) for Part d).

Conditions for the topic/eligibility criteria

Category-specific eligibility criteria:

a) Practitioner participation mandatory?: yes ☒ / no☐: from at least 8 Member States or Associated Countries

- Each proposal must include a plan, and a budget amounting at least 20% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions with a view to assessing the feasibility of their findings;
- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions (see in "Scope");

DRAFT

- Each proposal must include a workpackage to disseminate their findings, including an annual workshop;
- In 2017, only the disciplines not covered in 2016 will remain eligible. The list of disciplines excluded from the 2017 Call will be provided to applicants.

b) Practitioner participation mandatory?: yes ☒ / no☐: from at least 8 Member States or Associated countries, including at least 1 from outside the region.

- Each proposal must include a plan, and a budget amounting at least 20% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions with a view to assessing the feasibility of their findings;
- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions (see in "Scope");
- Each proposal must include a workpackage to disseminate their findings, including an annual workshop;
- In 2017, only the geographical areas not covered in 2016 will remain eligible. The list of regions excluded from the 2017 Call will be provided to applicants.

c) Practitioner participation mandatory?: yes ☒ / no☐: from at least 8 Member States or Associated countries

- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions (see in "Scope");
- Each proposal must include a workpackage to disseminate their findings, including an annual workshop;
- Only one such network may be supported over the 2016-2017 period.

d) Proposals may only include NCPs from EU Member States, Associated Countries and Third Countries that have been officially appointed by relevant national authorities. The consortium should have a good representation of experienced and less experienced NCPs from at least 8 Member States or Associated Countries

- EU Member States or Asssociated Countries choosing not to participate as a member of the consortium should be identified, and the reason for their absence must explained in the proposal;
- No more than one such network may be supported, in 2017.

DRAFT

Conditions for the CALL – SECURITY

Publication date: 25 March 2016 for the 2016 call and 25 March 2017 for the 2017 call

Deadline: XX at 17:00 hours Central European Time for the 2016 call and XX at 17:00 hours Central European Time for the 2017 call

Indicative budget :

	2016 EUR million	2017 EUR million	
Topics:		----------	All single stage
Topics:	----------		All single stage

Eligibility conditions:

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

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

Evaluation criteria:

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

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

- Proposal page limits and layout: 70 pages

- Indicative timetable for evaluation and grant agreement[6]: [as appropriate]

- specify planned date to inform applicants of outcome of evaluation, and

- indicative date of signature of grant agreements or notification of grant decision

	Information on the outcome of	Indicative date for the signing of

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

	the evaluation (single or first stage)	grant agreements
Topics:	XX	XX
Topics:	XX	XX

Consortia agreements: [as appropriate]

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

DRAFT

SEC – GM 2 – 2016 and 2017: SME Instrument

Full details on the continuously open SME instrument call (*H2020-SMEInst-2016-2017*) are provided under the Horizon 2020 Work Programme Part – Innovation in SMEs (Part 7 of this Work Programme).

This Work Programme part contributes the following challenge of the SME instrument call:

SMEInst-*XX*-2016-2017: Engaging SMEs in security research and development
Specific challenge: To engage small and medium enterprises in security research and development, especially those not traditionally involved in it, and reduce as much as possible the entry barriers to SMEs for Horizon 2020 funding.

The actions under this topic could cover any aspect of the Specific Programme for "secure societies - protecting freedom and security of Europe and its citizens" (Horizon 2020 Framework programme and Specific programme), with the exception of point "7.4. Improving cyber security", which is covered by the SME instrument topic XXXXX.

Budget:

	2016 Budget EUR million	*2017 Budget EUR million*
Contribution from this part to call '*H2020-SMEInst-2016-2017*' (under Part 7 of the work programme)	*€9.374.685,25*	*€10.169.470,01*

SEC – GM 3 – 2016 Fast track to Innovation – Pilot

Full details on this pilot are provided in the separate call for proposals under the Horizon 2020 Work Programme Part - Fast Track to Innovation Pilot (Part 18 of this Work Programme)

DRAFT

CALL – DIGITAL SECURITY

[DRAFT] Overview of the Digital Security Focus Area activities in SC7, SC1 and also indicate where security and/or privacy research is called for in other topics within LEIT-ICT, including the specific activities on security. The text will be drafted as soon as the structure and content of the related WPs and Topics are finalised.

ICT-driven transformations bring opportunities across many important sectors but also vulnerabilities to critical infrastructures and services, which can have significant consequences on the functioning of society, economic growth and the technological innovation potential of Europe. These challenges are being addressed through innovative approaches that transverse the boundaries of individual H2020 pillars, calls and challenges.

Therefore, apart from the topics presented here, several relevant research & Innovation activities in Digital Security are foreseen in other areas of the 2016-2017 H2020 Work Programme.

- Topics in LEIT-ICT, in particular ICT 8.1, 8.2 and 8.3
- Societal Challenge 1: PM 20 – 2016 - Increasing digital security of health related data on a systemic level

DRAFT

DS1 – 2016: Cyber Security for SMEs, local public administration and Individuals

Specific Challenge:
Europe's SMEs, local public administration and citizens face particular challenges in addressing basic cyber security threats.

On one hand, in the case of SMEs and local public administration, their size and budgetary constraints often precludes them from putting in place highly granular organisational structures, retaining dedicated information security personnel and making significant investments in cybersecurity products or services.

Individuals, constantly portrayed as the "weakest link" face the daunting task of having to constantly adapt their behaviour at home and in the workplace and the way they use both their personal or work-related IT equipment and devices in order to avoid falling prey to the latest threats and techniques that malicious actors leverage against them.

Moreover, whether addressing SMEs, local public administrations or individuals, few cyber security solutions have been designed with the human factor in mind and therefore present severe limitations in their usability which hampers proper decision making and adequate usage.

Scope:

a. Innovation Actions
Taking into consideration the adequate level of security commensurate with the considered use-case, proposals may address one of the following types of end-users:

- SMEs,
- local public administration,
- individual citizens,.

To identify the most wide spread threats and cyber security issues facing end-users, proposals should take into account the guidance documents, best practices and standards issued by International Standardisation Organisations, technical forum and Member State Authorities which are tailored for SMEs or Individuals and actively contribute to their development or improvement.

Proposals should develop innovative solutions with a high degree of usability and automation while ensuring that the end-users retain an adequate degree of cyber situational awareness and control.

Factors going beyond technological solutions and focusing on psychological and behavioural factors that affect cyber security at individual or organizational levels should be addressed.

Proposals are expected to validate their work through extensive end-user feedback and participation in the consortium where appropriate.

Proposals have to address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users.

Expected Impact:
At macro level:

- Increased competiveness of European ICT security products and services catering to the needs of SMEs, local public administrations and individuals.

At societal level:

DRAFT

- Increased resilience against widespread cyber security threats facing SMEs, local public administrations and individuals.

At research and innovation level:

- Increased effectiveness of cybersecurity solutions through usability advancements and increased automation.

Type of instrument(s):

a. **Innovation Actions**, TRL 5-7.Proposals requesting contributions between 3 and 4 MEUR are expected.

Budget per type of instrument(s):

a. Innovation Actions: 20MEUR

DRAFT

DS2 – 2016: Economics of Cybersecurity

Specific Challenge:

Many cyber security failures in systems and organisations can only be explained and appropriately addressed by examining the problem through not only from the technical point of view but also through a deep societal, institutional and economic analysis.

Moreover, current structures at institutional level (national and international) as well as incentive frameworks (financial or regulatory, positive or negative) don't seem to be able to provide adequate coverage to threats.

Scope:

a. Research and Innovation Actions

With a multidisciplinary approach combining economic, behavioural, societal and engineering insights, measurement approaches and methodologies and combining methods from microeconomics, econometrics, qualitative social sciences, behavioural sciences, decision making, risk management and experimental economics, proposals are expected to cover one of the following two strands:

- Cybersecurity cost-benefit framework:
  - Security and privacy cost models including the pricing of digital assets, modelling and methods for estimation of costs of intangible risks (reputation, non-critical service disruption…) and relevant metrics and indicators;
  - The proposals should study and take into consideration relevant market sector specificities, and validate their models with relevant actors from these sectors.
  - Optimal investment in information security, risk management and cyber security insurance;

- Incentives and business models:
  - Identifying the incentives and striking the right balance between cooperative and regulatory approaches to information sharing regarding incidents and vulnerabilities;
  - Consider behavioural aspects of security and privacy;
  - Investigate the opportunities and risks of information security markets (e.g. bug bounties, vulnerability discovery & disclosure);
  - Develop revenue models for criminal activity and the deployment of cost-effective security measures as necessary disincentive for attacks and cyber-criminal activity.

For both sub-topics proposals should also investigate improvements and/or alternatives to current institutional and governance frameworks (market-driven as well as national and international regulatory) with a view to improving cybersecurity.

Based on their results, proposals should provide a set recommendations addressed to all relevant stakeholders including policy makers, regulators, law enforcement agencies (where applicable) as well as relevant market operators and insurance companies.

Expected Impact:

At macro level:

- Improved societal understanding of information security failures and how they should be addressed.
- Improved risk-based information security investment.

At societal level:

- Increased societal resilience to cyber security risks through more efficient and effective institutional and incentives structures.

At research and innovation level:

- Progress beyond the state of the art in information security economics models.

Type of instrument(s):

a. **Research & Innovation Actions**. One project requesting a contribution of between 1 and 2 MEUR is expected for each strand.

Budget per type of instrument(s):

a. Research and Innovation Actions: 4MEUR

DRAFT

DS3 – 2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Specific Challenge:

Recognising the increasing importance of securing our European Digital Society against cybersecurity threats, a significant increase in related Research and Innovation activities has been observed such as the development of local cybersecurity and privacy innovation clusters, as well as investment driven at regional and national level.In order to maximise thematic synergies between H2020, EU and national efforts in the area of cybersecurity R&I, a better overview of these activities is needed.

Globally, an exchange of views and possible cooperation around cybersecurity and privacy research and innovation approaches, policies and best practices with like-minded third countries is also necessary in order to bring relevant elements of comparison and allow European stakeholders (public and private) to actively participate in those discussions which will determine the future global cyber security landscape.

Scope:

Coordination and Support Actions Proposals may cover one of the strands identified below.

1. Synergies between H2020, EU Member States and associated countries R&I activities and cybersecurity innovation clusters.
   Proposals should address two main challenges:
   - Foster and promote European cybersecurity and privacy research and innovation
   - Maximise synergies between R&I actions at EU and national levels;
   - Proposals shall be of a 4 year duration to cover projects from 2014-2015 and 2016-2017 WPs.

   Proposals should therefore:
   - Identify Cybersecurity innovation clusters across EU Member States and promote their interaction and cooperation;
   - Map the cybersecurity and privacy end-users landscape and identify their specific needs which should be addressed through innovative solutions while taking into consideration all relevant prior work in this area (in particular from FP7 and CIP);
   - Organise an annual workshop bringing together participants from the EU clusters and participants in EU funded research and innovation projects;
   - In order to address both the technology supply and end-users demand side in cybersecurity and privacy, Digital Security and Privacy in ICT are recognised as challenges across individual H2020 pillars challenges and are addressed in many relevant R&I areas. For example, in LEIT-ICT these issues are addressed in embedded systems, micro-electronics, smart cards, 5G, cloud computing, big data, IoT…). In order to achieve maximum possible synergies and cross-fertilization between relevant research and innovation activities, it is needed to cluster the many projects encompassing security and privacy R&I into a Digital Security and Privacy Cluster for H2020;
   - Produce a detailed report of Member State national cybersecurity and privacy related Research & Innovation programmes and research agendas in order to identify the areas where EU funding may achieve maximum impact;
   - Identify new opportunities for cybersecurity innovation in Europe by looking at emerging trends and disruptive technologies (such as quantum cryptography);
   - Provide input into the work of the NIS Platform WG3 Strategic Research agenda, ENISA and national cybersecurity and privacy R&I road mapping initiatives at Member State level;
   - Identify and synthesize relevant policy, regulatory, economic, aspects including education and skills;

DRAFT

- Identify and support standardisation efforts of proposals in the Digital Security Calls and propose actions to be included in the European Commission's ICT Standardisation Rolling Plan.
- Identify and connect relevant market agents, capitalising on European strengths in the cybersecurity sector, including business drivers, technology enablers, and deployment challenges, from both supply and demand sides

2. International dialogue with Japan
   - Encourage and facilitate an exchange of views between the relevant EU and Japanese stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges; identify and map the relevant legislation and policies in place stimulating the innovation and deployment of cybersecurity solutions.
   - Support the EU-Japan ICT dialogue in the area of cybersecurity;
   - Identify opportunities for future cooperation between the European research and innovation ecosystems (including standardisation) and policy makers and the corresponding institutional and private Japanese entities.
   -

3. International dialogue with the USA
   - Encourage and facilitate an exchange of views between the relevant EU and the US stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges; identify and map the relevant legislation and policies in place stimulating the innovation and deployment of cybersecurity solutions.
   - Identify opportunities for future cooperation between the European research and innovation ecosystems (including standardisation) and policy makers and the corresponding federal and private US entities.
   - Launch a multistakeholder reflection between European and US institutional, research and think tanks addressing the international, technical as well as socio-political challenges in cybersecurtity;

Expected Impact:
At macro level:
- Identify and prioritise R&I topics across the EU.
- Foster and promote European cybesecurity innovation activities
- Increase the international visibility of EU activities in cybersecurity.

At societal level:
- Identify potential European and international common approaches in addressing cybersecurity challenges from a R&I as well as a governance and institutional perspective.

Type of instrument(s):
Coordination and Support Actions: Three Actions will be funded: 1 for each strand.

Budget per type of instrument(s):
Coordination and support Actions: 1MEUR for strand 1., 0,5MEUR for strand 2 and 0,5 MEUR for strand 3.

DRAFT

DS4 – 2017: Addressing Advanced Cyber Security Threats and Threat Actors

Specific Challenge:

Over the past decade, we have seen that cyber attacks have become increasingly sophisticated, stealthy, targeted and multi-faceted which may leverage zero-day exploits and highly creative interdisciplinary attack methods.

Detecting and responding to such attacks by a highly motivated, skilled and well-funded attacker has however been proven highly challenging.

As our society is becoming increasingly dependent on (critical) cyber infrastructure, new technologies are needed to increase our detection and response capabilities.

Scope:

a. Research and Innovation Actions –Situational Awareness

The focus of the proposals should be on the development of novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks.

The solution may leverage techniques such as anomaly detection, visualisation tools, big data analysis, threat analysis, deep-packet inspection, protocol analysis, etc as well as interdisciplinary research to counter threat actors and their methods.

The proposals should also consider the need to collect necessary forensic information from attackers that can be used as evidence in court.

Proposals are encouraged to assess and address the the impact to fundamental rights, data protection and privacy in particular, in the design and developmentof their solutions.

b. Innovation Actions – Simulation Environments, Training

Proposals should develop innovative simulation environments and training materials in order to adequately prepare those tasked with defending high-risk organisations to counter advanced cyber-attacks.

The simulation environments should take into consideration the following challenges:

- Tools for creating realistic cyber environments that fit the training objectives and tools for producing both benign and malicious system events that fit the training scenario;
- Real-time student performance assessment, dynamic configuration and adaptation of exercise scope and difficulty;
- Exercise monitoring and evaluation of its state, being able to control the progress of the exercise, detect inconsistencies and hard-to-solve situations, etc;
- Definition and creation of new scenarios and cyber threats in a cost and time-effective manner, and that better achieve the pedagogical objectives for a wide variety of student profiles;

In the context of cyber security attacks, proposals may also consider scenario building and simulation training to prepare organisations' response and decision making processes in relation obligations stemming from applicable legal frameworks or in the wider context of managing crises and emergency situations.

Proposals have to address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users.

Expected Impact:

At macro level:

- Improved detection and response time to advanced cyber security threats.

At societal level:

- Increase society's resilience to advanced cyber security threats.

At research and innovation level:

- (RIA) Progress in technologies and processes needed to improve organisations' capabilities to detect and respond to advanced attacks.
- (IA) Improvements in the preparadness of those charged with defending ICT systems from advanced threats in high risk scenarios.

Type of instrument(s):Type of instrument(s):

a. **Research & Innovation Actions**. TRL 3-5. Proposals requesting a contribution of between 2 and 3 MEUR are expected.

b. **Innovation Actions**, TRL 5-7. Proposals requesting contributions between 4 and 5 MEUR are expected.

c. Coordination and Support Actions

Budget per type of instrument(s):

a. Research and Innovation Actions: 10MEUR

b. Innovation Actions: 10MEUR

DRAFT

DS5 – 2017: Privacy and Data Protection and Digital Identities

Specific Challenge:

The use of modern telecommunications and on-line services involve users' personal information.. For example, using search engines exposes the query terms used, which can be both sensitive and identifying, as illustrated by the exposure of search terms; social networking services expect users to reveal their social connections, messages and preferences, that could lead to direct privacy violation if exposed. Browsing the web also leaves traces of where users have gone, their interests, and their actions - meta-data that can be used to profile individuals.

The implementation the draft General Data Protection Regulation (GDPR - currently in the law-making process) presents both technological as well as organisational challenges for organisations which have to implement novelties such as the right to data portability, the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability.

Many services on the Internet depend on the availability of secure digital identities which play a crucial role in safeguarding the data and privacy of citizens as well as protecting them and other actors such as private companies or public services form various online threats. At the same time, many European countries already have or are in the process of developing an electronic identity (eID) scheme. Most of these projects are built to be at a very high security level, which makes them very suitable for diverse eGovernment processes. But in turn they may lack usability for commercial applications.

Scope:

a. Innovation Actions: Proposals may cover one of the strands identified below.

- Privacy-enhancing Technologies (PET)

  Novel designs and tools to provide users with the functionality they require without exposing any more information than necessary, and without losing control over their data, to any third parties. PET should be available in a broad spectrum of products and services, with usable, friendly and accessible safeguards options. PET should be developed having also cost effective solutions.

  Comprehensive and consistent Privacy Risks Management Framework should be available, in order to allow people to understand their privacy exposure (i.e. helping people to understand what happens to their data when they go online, use social networks etc).

  Open source and externally auditable solutions are encouraged in order to maximise uptake and increase the trustworthiness of proposed solutions.

- General Data Protection Regulation in practice

  Tools and methods to assist organisations to implement the GDPR taking into account the final provisions of GDPR and guidance from relevant authorities (Data Protection Authorities, Art 29 WP or its successor).

  Proposals may also addrees the need to provide support (procedures, tools) for entities to understand how to operate without requiring unnecessary information (so as to promote privacy respecting practices), in particular when the issue is mainly related to the fact that organizations (businesses, service providers, and government agencies) often require too much information from their target customer/user.

- Secure digital identities

  With a view to reducing identity fraud while protecting the privacy of citizens, proposals should develop innovative, secure and privacy enhancing digital identity platforms beyond national eID systems.

  Activities may leverage existing European electronic identification and authentication platforms with clearly defined interfaces based on the General Data Protection Regulation (GDPR).

  Proposals may:

  - Leverage evidence-based identities (using adequate correlation of multiple soft proofs of identity, as opposed to the usage of a central register);

- Provide a function for so called "qualified anonymity", which means, that the online service does not have any information about the user but a pseudonym. The real identity of the user can only be revealed under specific conditions such as at the request of legal authorities;

Consider cost-effective and user-friendly verification methods for mobile identity documents.

Proposals should identify and address the societal and ethical dimensions of the strand they choose to cover taking into consideration the possibly divergent perspectives of pertinent stakeholders.

Proposals have to address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users.

Expected Impact:

At macro level:

- Support for Fundamental Rights in Digital Society.

At societal level:

- Increased Trust and Confidence in the Digital Single Market

At research and innovation level:

- Increase in the use of privacy-by-design prionciples in ICT systems and services

Type of instrument(s):

a. **Innovation Actions**. TRL 5-7. Proposals requesting a contribution of between 2 and 3 MEUR are expected.

Budget per type of instrument(s):

a. Innovation Actions: 21MEUR

DRAFT

Sub Call – Digital Security and SMEs

This Work Programme part contributes the following challenge of the SME instrument call:

SMEInst-XX -2016-2017: Innovative European SMEs in cybersecurity
Specific challenge: To engage small and medium enterprises in cybersecurity research and development, especially those not traditionally involved in it and reduce as much as possible the entry barriers to SMEs for Horizon 2020 funding.

The actions under this topic could cover any aspect of the Digital Security Call of the Specific Programme for "Secure societies - protecting freedom and security of Europe and its citizens" (Horizon 2020 Framework programme and Specific programme), e.g. cryptography, usable cybersecurity solutions for SMEs, privacy enhancing technologies, secure digital identity management, cyber threat detection, etc,with the exception of point topics DS2-2016 "Security Economics" and DS3-2016 "EU and International Coordination in Cybersecurity Research and Innovation" Improving cyber security.

BUDGET:

	2016 Budget *EUR million*	*2017 Budget* *EUR million*
Contribution from this part to call '*H2020-SMEInst-2016-2017*' (under Part 7 of the work programme)	*€9.000.000,00*	-

DRAFT

OTHER ACTIONS (NOT SUBJECT TO CALLS FOR PROPOSALS)

1 - 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 contribution to the SST programme will be realised through a grant to a predefined beneficiary resulting from the implementation of the programme to support the emergence of a SST capacity at European level.

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 grant agreement is to be concluded in 2015 in the context of the SST support programme, in which the designated beneficiary will be the consortium resulting from the implementation of the support programme for the emergence of a SST capacity.

Type of action: Predefined beneficiary - Research and innovation actions (100%)

Indicative budget: EUR 1 million from the 2016 budget and EUR 1.2 million from the 2017 budget

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

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

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

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

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

Indicative budget: EUR 0.25 million from the 2016 and EUR 0.25 million from the 2017 budget

DRAFT

3 – Evaluations of the proposals for the 2016 and 2017 calls "Critical Infrastructure Protection" and "Security"

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

Type of action: Coordination and Support Action – Expert contracts

Indicative budget: Up to EUR X.XX million from the 2016 and EUR X.XX million from the 2017 budget

4 – Evaluations of the proposals for the 2016 and 2017 calls "Critical Infrastructure Protection" and "Digital Security"

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

Type of action: Coordination and Support Action – Expert contracts

Indicative budget: Up to EUR X.XX million from the 2016 and EUR X.XX million from the 2017 budget

5 - 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. Several different contracts will be used including existing framework contracts.

Timeframe: Spread across from the first quarter of 2016 to the last quarter of 2017

Indicative budget: Up to EUR 1.5 million from the 2016 and up to EUR 1.5 from the 2017 budget for points a) and b); up to EUR x.y million from the 2016 and from the 2017 budget for point c)