ANNEX 17 TO THE DECISION

FIRST DRAFT VERSION

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

Note on the meaning of the "Impact" section:

The more the specific expected impacts can be expected from a project, the higher the mark of the proposal in respect to "Impact"

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

CALL – CRITICAL INFRASTRUCTURE PROTECTION

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

Specific challenge:

Disruptions in the operation of elements of our countries' infrastructure may put at risk the functioning of our societies and their economies. Such disruptions may result from 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 and other elements of the European critical infrastructure: A comprehensive, yet element-specific approach is needed to securing the integrity of existing or future, public or private, connected 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 elements of critical infrastructures: Water supply station; Nuclear power plant; Natural gas power plant; Coal power plant; Oil thermal power plant; Geothermal power plant; Solar power plant; Wind mill power plant; Means of transportation at maritime ports, train or metro stations, or airports; Pipeline; Tunnels.

Proposals should cover: prevention, detection, response, and in case of failure, mitigation of consequences (include novel installation designs) with a view to achieving the security and resilience of all functions performed by the installations. They not should not only address in details all aspects of both physical (e.g. bombing, plane or drone overflights and crashes, spreading of fires, floods, etc.) and cyber issues and incidents, but also the combinations of physical and cyber issues and incidents, and their cascading effects. .

Expected impact:

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure element.
- Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure element.
- Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure element.
- In situ demonstrations of efficient and cost-effective solutions.
- Security risk management plans integrating both physical and cyber aspects.
- Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure element.
- Test results and validation of models of a specific element of critical infrastructure against physical and cyber threats.

- Establishment and dissemination throughout the relevant user communities of element-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: yes ☒ / no☐ If yes how much?: around 10 MEUR

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

TRL level: 7

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐ ： The coordinator must be an operator of the chosen installation/part of critical infrastructure.

The participation of industry is required.

SME participation mandatory: yes ☒ / no ☐

Other specific eligibility criteria

In 2016 and 2017 only up to one project will be selected to address each of the elements of critical infrastructures listed in the “Scope” section of this topic.

In 2017 only the elements not covered in 2016 will remain eligible. A list will be provided to applicants.

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]*

CALL – SECURITY

Sub Call - Disaster-resilience: safeguarding and securing society, including adapting to climate change

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.

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 management are not sufficiently interlinked, which prevents efficient response planning and the building of realistic scenarios. Integrated tools need to be developed to support such actions. Stronger partnerships among research, policy, 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, radiological or environmental accidents; the IPCC[2] recommendations in relation to extreme climatic events; the Hyogo Framework for Action at international level.

Response to emergency situations resulting from the materialization of such risks requires 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 decision-makers 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 environments and situations.

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 post-Hyogo Framework for Action)
- Enhanced autonomy, mobility and resilience of rescue and first aid organisations in case of disasters, including in remote regions or in case of emergency situations during mass events
- Development of new tools, or networking of existing technologies (e.g. self-deploying and autonomous sensors) that are useful for response planning and scenario building, including e.g. modular concepts and systems based on renewable energies, electric vehicles, mobile power 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 compliant with EU guidelines and recommendations
- Development of tools enhancing population awareness and involvement
- Enhanced cooperation between sea-, land- and air-based systems
- Assessment of the societal acceptance of such tools, also from an ethical point of view.
- Greater cooperation among actors involved in crisis management
- Greater implications of practitioners (e.g. first responders) in validating and testing of tools and methodologies

[2] Intergovernmental Panel on Climate Change

General aspects of the topic

Innovation Action

Budgetary indication for proposers: yes ☒ / no☐: about 8 MEUR

International cooperation: yes ☒ / no ☐

TRL level: TRL 7 or 8

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐ : 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 ☐

SEC - DRS 2 - 2016: PCP of 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.

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, search and rescue, communication), result from public-private cooperation, and demonstrate resiliency 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, etc.)

The buyers will:

Phase 0: 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;

Phase 1: Plan and implement these tender procedures for eventually acquiring two prototypes of the system, from two different sources;

Phase 3: Test and validate the prototypes of the system;

Phase 4: Demonstrate the prototypes of in two multidisciplinary (firefighters, medical emergency services, police departments, etc.), international (involving practitioners from at least 4 Member States or Associated Countries), and realistic scenarios of different nature.

Expected impact:

- Improved cooperation among civil protection services across the EU
- Improved exchange of experiences between (public) stakeholders on civil protection in relation to operations within the disaster risk management cycle (prevention, preparedness, surveillance, response);

Further to the PCP's successful achievement, the European Commission may consider launching a PPI to facilitate the acquisition of operational systems satisfying the specifications established within the PCP, possibly in synergy with other EU-funding instruments.

[3] Decision 1313/2013

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: yes ☒ / no☐: about 10 MEUR

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

International cooperation: yes ☒ / no ☐

SME relevant: yes ☒ / no ☐

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

Conditions for the topic/eligibility criteria

Proposals must necessarily state:

1) the participants' agreement to negotiate in good faith and on a case by case basis, licenses to any and all of their to the background necessary for the implementation and use of the contents of the standards, specifications, design, research roadmaps, tender packages or other documents generated in the action.

2) the participants' commitment that all such licenses shall be according to Fair, Reasonable and Non-Discriminatory ("FRAND") terms."

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 between 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 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) 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-) agents, 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 measurement techniques, including sample preparation strategies and analyses made in-situ issued by mobile 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, in-situ analyses and technical approaches for forensic analysis, for the detection and identification of biological toxins;
- 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

Budgetary indication for proposers: yes ☒ / no☐: up to 8 MEUR

International cooperation: yes ☒ / no ☐

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

SEC- DRS 4 - 2017: PCP for 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:

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

Phase 1 to 4

If the above-mentioned CSA has foreseen to go directly along the way of procurements:

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: yes ☒ / no☐ 10 MEUR to 15 MEUR

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

TRL level: 8

Conditions for the topic/eligibility criteria

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

If no Phase 0 is necessary, proposals must involve buyer organizations from at least 8 EU Member States

Proposals must necessarily state:

1) the participants' agreement to negotiate in good faith and on a case by case basis, licenses to any and all of their to the background necessary for the implementation and use of the contents of the standards, specifications, design, research roadmaps, tender packages or other documents generated in the action.

2) the participants' commitment that all such licenses shall be according to Fair, Reasonable and Non-Discriminatory ("FRAND") terms."

Practitioner participation mandatory?: yes ☒ / no☐ : Minimum condition for PCP

SEC - DRS 5 - 2016: CBRN cluster

[STILL NOT MATURE ENOUGH]

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 to also avoid aviation related threats.

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. 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, political, propaganda-, media- or internet-based. Events and conditions leading a person from ideas to violent action are also numerous.

Radicalised individuals, Europeans or foreigners, get organized in various ways: centralised and hierarchical organisations; smaller groups based in Europe or on foreign territories; cells; and lone actors operating in a more unconstrained and unpredictable way.

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.

Expected impact:

- Deeper knowledge of the main constituents of the processes of violent radicalisation ;
- Better ability to detect and prevent radicalisation by national and local security practitioners in a timely manner;
- Compared 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;
- 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: yes ☒ / no☐ If yes how much?: 2 MEUR to 3 MEUR

Ring-fenced budget for the topic?: yes ☒ / no ☐ If yes how much?: 6 MEUR

Possible classification: 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.

SEC - FCT 2- 2017: Human Factor for 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 cyber criminality to develop, and corruption and financial crime to take new forms. Cyber criminality is a relatively new phenomenon, which is not satisfactorily understood, nor properly addressed. The same applies to the innovative technologies and methodologies for financial crimes

Expected impact:

The EU law enforcement agencies will benefit from improving and consolidating knowledge about security problems and their remedies.
In detail:

- A policy 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

[4] Internal Security Strategy for the European Union: "Towards a European Security Model", Council of the European Union, 7120/10

- Better understanding of how the citizens perceive security and how it affects their feeling of insecurity, 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, including:
    - New methods for de-escalation during mass gatherings.
    - New methods to prevent, investigate and mitigate cybercriminal behaviours.
    - New methods to prevent, investigate and mitigate corruption and financial criminal behaviours.

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: yes ☒ / no☐ If yes how much?: 3 MEUR to 4 MEUR

Ring-fenced budget for the topic?: yes ☒ / no☐If yes how much?: 8 MEUR

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

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, in general:

- Advanced methods for data analysis and statistical interpretation of evidence;
- Prototype infrastructure for the secure transmission of legally opposable data to and from forensic experts in the field or in laboratories, for data analysis/interpretation and reporting back to the relevant actors;
- Curricula for training forensic investigators to use these new technologies;
- Methodologies to compare results produced by forensic organizations across Europe (to ensure EU-wide consistency of forensic work.)

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 past 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 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.)

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: yes ☒ / no☐ If yes how much?: 3 MEUR to 5 MEUR

Ring-fenced budget for the topic?: yes ☒/ no☐ If yes how much?: 10 MEUR

Only 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

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

Specific challenge:

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; To draft a curriculum for pan European training in forensic technologies, and to plan for its assessment across Europe;

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 propose a realistic EU-wide certification mechanism for forensic techniques and tools based on the benchmarks and validation methods above.

Expected impact:

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

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 10 MEUR to 15 MEUR

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

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

Other specific eligibility criteria:

Proposals must necessarily state:

1) the participants' agreement to negotiate in good faith and on a case by case basis, licenses to any and all of their to the background necessary for the implementation and use of the contents of the standards, specifications, design, research roadmaps, tender packages or other documents generated in the action.

2) the participants' commitment that all such licenses shall be according to Fair, Reasonable and Non-Discriminatory ("FRAND") terms."

SEC - FCT 5- 2016: 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). 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: yes ☒ / no☐ If yes how much?: 5 MEUR to 10 MEUR

Ring-fenced budget for the topic?: yes ☒ / no☐ If yes how much?: 15 MEUR

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

Practitioner participation mandatory?: yes ☒ / no☐: At least two 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.).

SEC - FCT 6 - 2017: Detection techniques on explosives: Countering the use of 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; improve or bring to higher TRLs existing methods and techniques, and their use 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 (including in transit);
- Neutralization of IED;
- Identification of weakness of the current defences against IED, and possible improvements.

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.
- 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: yes ☒ / no☐ If yes how much?: 4 MEUR to 6 MEUR

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

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.

SEC - FCT 7- 2016: 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. virtual/crypto currencies des-anonymisation/tracing/impairing where they support underground markets in the darknet (e.g. Deep Web);
    Sub-topic: 2. rogue/suspicious light drone/UAV flying over restricted areas;
    Sub-topic: 3. [one or 2 more sub-topics could be added]
    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 agents 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: yes ☒ / no☐ If yes how much?: 3 MEUR to 5 MEUR

Ring-fenced budget for the topic?: yes ☒ / no☐ If yes how much?: 10 to 15 MEUR

TRL level: **7**

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐:

- In the Sub-topics made explicit in the scope of the topic: a minimum of 3 LEA from 3 EU Member States

- 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.

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, exploiting the full potential of EUROSUR and promoting an enhanced use of new technology for border checks, also in relation to the Smart Borders legislative initiative. It also addresses supply chain security in the context of the EU's customs policy.

On the other hand this 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.

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, 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.

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 in different framework conditions.

Phase 3: By 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, 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.
- Improved management of EU resources' allocated to EU civilian external actions.

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 10 MEUR to 15 MEUR

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

Possible classification: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: 7

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: a minimum of three from three different EU Member States

Other specific eligibility criteria:

Proposals must necessarily state:

1. the participants' agreement to negotiate in good faith and on a case by case basis, licenses to any and all of their to the background necessary for the implementation and use of the contents of the standards, specifications, design, research roadmaps, tender packages or other documents generated in the action.

2. the participants' commitment that all such licenses shall be according to Fair, Reasonable and Non-Discriminatory ("FRAND") terms."

SEC - BES 2 – 2016: Towards cost reduction in land border security applications

Specific challenge:

As international travel flows continue to rise, the pressure to process large volumes of people at the borders keeps growing. Border management in European Union context means first and foremost the enforcement of the common policies and implementation of the common rules.
However, the external borders of the European Union land borders (and border crossing points) present a wide range of very different areas, ranging at from those of Nordic Countries to those of Greece (rivers, forests, mountains, agricultural and urban areas….).

The European Border Surveillance System (EUROSUR) has established a mechanism for Member States' authorities carrying out border surveillance activities to share operational information. 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. Innovative, cost-efficient technologies are needed, or existing ones need to become more affordable, to meet border authorities and practitioners' 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 places bearing the heaviest burden (based on the analysis of flows of people, 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;

The availability or scarcity of human resources is another parameter to be taken into account when considering the added value and cost of novel technologies solutions.

Overlap with the work being undertaken by border surveillance authorities in the context of the EWISA project should be avoided.

Expected impact:

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

- 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, training requirements for new skills, etc.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 5 MEUR to 10 MEUR

Possible classification: yes ☒ / no ☐

SME relevant: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **6**

Practitioner participation mandatory?: yes ☒ / no☐: At least 2 from 2 different EU Member States

SEC - BES 3 - 2016: 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. The current effectiveness of checks could remain unchanged if thorough screening could be limited further to a preliminary (and non-disruptive) risk-based analysis of the individual goods and people in the flows.

Scope:

Proposals should take account of the four-tier access control model developed in the EU: measures in third countries; cooperation with neighbouring countries; border control 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 the field of transport safety may lead to the development of new solutions.

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;
- Improved border automated screening systems.

General aspects of the topic

Innovation Action

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 8 MEUR to 10 MEUR

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

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 from 2 EU Member States

SEC - BES 4 – 2016: Through-foliage detection, including in the outermost regions of the EU

Specific challenge:

The European Border Surveillance System (EUROSUR) has established a mechanism for Member States' authorities carrying out border surveillance activities to share operational information. But several regions at the borders of the European Union are covered with forests. 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 across the border with, for instance, Turkey, Ukraine 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 of all kind, and arrays of sensors 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.

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.

Expected impact:

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

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 5 MEUR to 10 MEUR

Possible classification: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **5 or 6**

Practitioner participation mandatory?: yes ☒ / no☐: At least 2 from 2 EU Member States

SEC - BES 5 - 2016: Architectures organization, data analysis and risk assessment for ensuring security in the supply chain

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 EU legal, procedural and IT systems where they exist. Realistic methodologies and organisations need to develop, that facilitate collaboration among the relevant authorities.

Common repositories that take advantage of existing instruments such as the Advance Cargo Information System (advance 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.

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.

- Reduction of terrorist threats; illicit trading of arms; illicit trading, in general, and counterfeiting; drug trafficking; human trafficking;

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

- 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, expected to reduce access costs for traders.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 4 MEUR to 6 MEUR

Ring-fenced budget for the topic?: yes ☒ / no☒ If yes how much?: 10 MEUR

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: At least 2 from 2 EU Member States

SEC - BES 6 – 2016: Acceptance of "no gate crossing point solution"

Specific challenge:

For the traveller it would be ideal to get through 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 for law abiding and honest people, whilst permitting to catch offenders at border crossing points. However, in the intensive use of technologies that this will require bears the risk to invading people's privacy, and the social and political acceptance of technologies for "no gate solutions" is required prior to their implementation.

Scope:

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. The assessment of the acceptability of such (combinations of) technologies and systems by citizens and practitioners is needed.

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:

- A method, and metrics, on the social acceptability of the concept of border control processes based on "no gate crossing point solutions", and of the various technology components that may be required.
- Information systems that better manage personal information and support the automated checking and analysing of entry and exit data, without increasing the risk of loss of privacy.
- Networks of sensors that better collect information needed for border checks, without increasing the risk of loss of privacy.

General aspects of the topic

Coordination and Support Action

Budgetary indication for proposers: yes ☒ / no ☐ If yes how much?: 2 MEUR to 4 MEUR

Ring-fenced budget for the topic?: yes ☒ / no ☐ If yes how much?: 7 MEUR

Possible classification: yes ☒ / no ☐

International cooperation: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

Practitioner participation mandatory?: yes ☒ / no☐: At least 2 from 2 EU Member States

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 exist, coming from different sources and for different security purposes, in a variety of formats, are available but not necessarily exploitable because not accessible at the same time, 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. 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;
- 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;
- 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).

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 have touched upon the issue.

Data fusion may bear on, or generate information needing classification.

Expected impact:

- Contribution to the development of EUROSUR and to the implementation of the EUMSS action plan.
- Improved border surveillance systems in terms of information exchange, situational awareness, and decision-making and reaction capabilities;
- Solutions better fitting the actual concepts of operations set for missions involving several Member States maritime border surveillance, security and search-and-rescue organisations;
- Solutions demonstrated in the context of interagency and cross-border cooperation;
- Solutions interfaced with existing infrastructure.

General aspects of the topic

Research and Innovation Action

Budgetary indication for proposers: yes ☒ / no☐ If yes how much?: 4 MEUR to 6 MEUR

Ring-fenced budget for the topic?: yes ☒ / no☐ If yes how much?: 10 MEUR

Possible classification: yes ☒ / no ☐

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

Possible synergies with EDA: yes ☒ / no ☐

TRL level: **6 or 7**

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

Other specific eligibility criteria: Participation from at least 2 independent industry organizations established in 2 different EU Member States is mandatory.

SEC - BES 8 – 2016 and 2017: PCP of systems to support maritime security

Specific challenge:

Regulation No 1052/2013 established the European Border Surveillance System (EUROSUR). EUROSUR promotes the establishment of a shared IT platform that enables participating authorities to instantly see and assess situations at and beyond the EU external border, with three layers of information – events, operational information, and analysis. However, most European maritime security operations today are supported by a mix of heterogeneous (information and detection) systems, deployed by a variety of organizations with different missions, and in several countries. The lack of interoperability or homogeneity of these systems is of major concern.

Scope:

Technologies and innovation may improve the above-described situation. Potential buyers of any kind of system[5] used primarily for maritime security operations could join to finance the production of prototypes that demonstrate the interoperability of existing systems, or that satisfy the full extent of requirements common to the largest set of buyers, whilst increasing interoperability with the EUROSUR IT platform.

The buyers will:

Phase 0: 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;

Phase 1: Plan and implement these tender procedures for eventually acquiring two prototypes of the system, from two different sources;

Phase 3: Test and validate the prototypes of the system

Phase 4: Demonstrate the prototypes of in a multidisciplinary (coast guards, navies, civil protection, etc.), international (involving practitioners from at least 4 Member States or Associated Countries), and realistic scenario.

Expected impact:

- Contribution to EUROSUR
- Interoperable or homogeneous systems to support maritime security operations, ready for industrialisation and of interest to practitioners in many EU countries.

Further to the PCP's successful achievement, the European Commission may consider launching a PPI to facilitate the acquisition of operational systems satisfying the specifications established within the PCP, possibly in synergy with other EU funds.

General aspects of the topic

Pre Commercial Procurement

Budgetary indication for proposers: yes ☒ / no☐ 8 MEUR to 12 MEUR

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

TRL level: **8**

Conditions for the topic/eligibility criteria

[5] For instance: [TO BE COMPLETED]

Practitioner participation mandatory?: yes ☒ / no☐ Minimal condition for PCP

Other specific eligibility criteria:

- The buyers must explicitly commit to provide in cash more than 30% of the budgeted cost of the action.

- The proposed systems must aim at achieving interoperability with the EUROSUR IT platform.

- Proposals must necessarily state:
  1) the participants' agreement to negotiate in good faith and on a case by case basis, licenses to any and all of their to the background necessary for the implementation and use of the contents of the standards, specifications, design, research roadmaps, tender packages or other documents generated in the action.
  2) the participants' commitment that all such licenses shall be according to Fair, Reasonable and Non-Discriminatory ("FRAND") terms."

[OPTION] Sub Call – Detection

This sub-call brings together the various topics of this Work Program which address the issue of detection tools and techniques, irrelevantly of their field of application (FCT, BES, DRS).

Considering the present version of this document, it would include:

[OPTION] SEC - BES 4 – 2016

[OPTION] SEC - FCT 6 - 2017

[OPTION] SEC - FCT 5- 2016

[OPTION] SEC - DRS 3 - 2016

[OPTION] SEC - DRS 5 – 2016

which would be deleted from BES, FCT and DRS sub-calls.

Sub Call - General Matters

SEC – GM1 – 2016 and 2017: Pan European Networks of practitioners and other actors in the field of security

Specific challenge:

In Europe, practitioners in the field of security 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. 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 network in various manners:

a) Practitioners **in the same discipline and from across Europe** (e.g. firefighters, police organisations, medical emergency services, 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 **from different disciplines** and concerned with current or future security or disaster risk and crisis management issues **in a particular geographical area** (e.g. the Mediterranean Sea, the Artic, the Danube River Basin) 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

c) Entities from **around Europe** that manage **demonstration and testing sites, training facilities, 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 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.

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 dedicated to other aspects of their work (in general, to the coordination of their operations).

General aspects of the topic

Coordination and Support Action

International cooperation: yes ☒ / no ☐

SME relevant: yes ☒ / no ☐

Possible synergies with EDA: yes ☒ / no ☐

Conditions for the topic/eligibility criteria

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

Other specific eligibility criteria:

- 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 the findings;
- Each proposal must include a plan, and budget at least 10% 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;
- In 2017, only the categories of practitioners not covered in 2016 will remain eligible. An exclusion list will be provided to applicants.

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: 120 pages [TBC]

- 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]

[OPTION 1] SEC – GM2 – 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:

SME instrument topic: "Protection of urban soft targets and urban critical infrastructures"

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

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

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

The critical infrastructures sectors listed in the European Programme for Critical Infrastructures Protection (EPCIP)[7], including, among others, energy installations and networks, communications and information technology, finance (banking, securities and investment), water (dams, storage, treatment and networks), supply chain and government (e.g. critical services, facilities, information networks, assets and key national sites and monuments) are not only relevant at a national scale but they can be considered critical infrastructures in an urban context as well.

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

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

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

– high throughput screening of people and their bags including the ability to screen them in reasonably real-time as people approach entrances to buildings or enter public transportation system;

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

- high throughput screening for vehicles to identify threats that warrant further inspection (as opposed to random searching);
- potential CBRN-E threats and the way in which these threats could be carried-out against soft targets and critical infrastructures;
- mitigation of vehicle-borne improvised explosive devices (IED), with a specific focus on vehicle-borne ones (e.g. in cases of parked vehicles, penetrative attacks, etc.).

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

Type of action: SME instrument 70% funding

[OPTION 2] SEC - GM2 – 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 – GM3 – 2016 and 2017 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)

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 known.

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 x,y,z
- Societal Challenge 1: PM 20 – 2016 - Increasing digital security of health related data on a systemic level

DS1 – 2016: Cyber Security for SMEs and Individuals

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

On one hand, in the case of SMEs, 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 on the other hand, constantly portrayed as the "weakest link", face the daunting task of having to constantly adapt their behaviour 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, few cyber security solutions have been designed with the human factor in mind and present therefore severe limitations in their usability which hampers proper decision making and adequate usage.

Scope:

a. Innovation Actions
To identify the most wide spread threats facing SMEs and individuals, 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 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 may choose to address the needs of SMEs, Individuals or both.

b. Coordination and Support Actions
To complement the research and innovation activities in this topic, support and coordination actions should address the following:
- Support the integration of results coming from the various projects related to this topic in order to provide an overall view of the area;
- Support dissemination (including the organisation of an annual domain workshop) and the production of relevant material synthesizing the R&I activities
- Identify and support liaison with relevant projects in other areas within H2020
- Support the standardisation efforts of the RIAs;
- Coordinate with relevant efforts undertaken by standardisation organisations and technical fora; Identify and propose actions to be included in the European Commission's ICT Standardisation Rolling Plan.
- Contribute to the related areas of the Strategic Research Agenda of the NIS Platform Working Group 3 (WG3) and other related research road-mapping activities;

Expected Impact:

At macro level:

- Increased competiveness of European ICT security industry catering to the needs of SMEs and Individuals.

At societal level:

- Increased resilience against widespread cyber security threats facing SMEs and Individuals.

At research and innovation level:

- Improvement in effectiveness of cybersecurity solutions through advances in their usability.

Type of instrument(s):

a. **Innovation Actions**, TRL 5-7.Proposals requesting contributions between 3 and 4 MEUR are expected.
b. **Coordination and Support Actions:** 1 CSA will be funded

Budget per type of instrument(s):

a. Innovation Actions: 16,5MEUR
b. Coordination and Support Actions: 0,5MEUR

DS2 – 2016: Security Economics

Specific Challenge:

Many cyber security failures in systems and organisations can only be explained and appropriately addressed by examining the problem through economics.

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 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 may address areas such as:

- Costing models including the pricing of digital assets and the costing of more intangible risks (reputation, non-critical service disruption…);
- Optimal investment in information security, risk management and cyber security insurance;
- Security and privacy models and metrics;
- Behavioural security and privacy;
- Information security markets (e.g. bug bounties, vulnerability discovery, disclosure).

Proposals should also investigate improvements and/or alternatives to current institutional and incentive 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 aimed at policy makers.

b. Coordination and Support Actions

To complement the research and innovation activities in this topic, support and coordination actions should address the following:

- Support the integration of results coming from the various projects related to this topic in order to provide an overall view of the area;

- Support dissemination (including the organisation of an annual domain workshop) and the production of relevant material synthesizing the R&I activities
- Identify and support liaison with relevant projects in other areas within H2020;
- Identify future standardisation needs and coordinate with relevant efforts undertaken by standardisation organisations and technical fora; Identify and propose actions to be included in the European Commission's ICT Standardisation Rolling Plan.
- Contribute to the related areas of the Strategic Research Agenda of the NIS Platform Working Group 3 (WG3) and other related research road-mapping activities;

Expected Impact:

At macro level:

- Improved 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**. TRL 3-5.Proposals requesting a contribution of between 2 and 3 MEUR are expected.
b. **Coordination and Support Actions**. 1 CSA will be funded.

Budget per type of instrument(s):

a. Research and Innovation Actions: 10MEUR
b. Coordination and Support Actions: 0,5MEUR

DS3 – 2016: EU and International Coordination in Cybersecurity Research and Innovation

Specific Challenge:

Recognising the increasing importance of securing our Digital Society against cybersecurity threats, a significant increase in related Research and Innovation activities has been observed such as the development of local cybersecurity industrial clusters, as well as investment driven at regional and national level in Europe.

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. Cooperation around cybersecurity research and innovation approaches, policies and best practices with like-minded third countries is also necessary in order to bring relevant elements of comparison.

Scope:

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

1. Coordination with EU Member States R&I activities and cybersecurity clusters
    - Produce a detailed report of National cybersecurity related Research & Innovation programmes and initiatives;
    - Identify Cybersecurity clusters in EU Member States;
    - Organise an annual workshop bringing together participants for the EU clusters;
    - Cooperate and coordinate with the Coordination and Support Action launched as a result of the LEIT-ICT8.2 – 2016 topic "Preparing the future of cybersecurity in Europe" providing input into the work of the NIS Platform WG3 Strategic Research agenda.

2. International coordination with Japan
    - Facilitate an exchange of views between the EU and Japan on matters relating to cybersecurity R&I.
    - Identify opportunities for cooperation between the European research and innovation ecosystems (including standardisation) and the Japanese R&I ecosystems.

Expected Impact:

At macro level:

- Identify and prioritise R&I topics across the EU.
- Foster a European cybesecurity industry
- Increase the international visibility of EU activities in cybersecurity.

At societal level:

- A coordinated European and international approach to addressing cybersecurity risks.

Type of instrument(s):

Coordination and Support Actions: Two Actions will be funded: 1 for each strand.

Budget per type of instrument(s):

Coordination and support Actions: 1MEUR

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

Specific Challenge:

Over the past decade, we have seen that attacks on cyber infrastructure have become increasingly sophisticated, stealthy, targeted and complex multi-faceted attacks which may include 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 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.

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:

- Student monitoring and real-time performance assessment, being able to dynamically adapt the difficulty of the exercise as well as provide automated support and guidance
- 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.

c. Coordination and Support Actions

To complement the research and innovation activities in this topic, support and coordination actions should address the following:

- Support the integration of results coming from the various projects related to this topic in order to provide an overall view of the area;
- Support dissemination (including the organisation of an annual domain workshop) and the production of relevant material synthesizing the R&I activities
- Identify and support liaison with relevant projects in other areas within H2020
- Support the standardisation efforts of the RIAs;
- Coordinate with relevant efforts undertaken by standardisation organisations and technical fora;

- Identify and propose actions to be included in the European Commission's ICT Standardisation Rolling Plan.
- Contribute to the related areas of the Strategic Research Agenda of the NIS Platform Working Group 3 (WG3) and other related research road-mapping activities;

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:

- Progress in technologies and processes needed to improve organisations' capabilities to detect and respond to advanced attacks.

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: 10

b. Innovation Actions: 10

c. Coordination and Support Actions: 0,5 MEUR. 1 CSA will be selected.

DS5 – 2017: Privacy and Data Protection

Specific Challenge:

Modern telecommunications and on-line services expect users to expose a large amount of personal information to use them. 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, leading to possible direct privacy violation or de-anonymization; even merely browsing the web leaves traces of where users have gone, their interests, and their actions - meta-data that can be used to profile and further target them.

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.

Scope:

a. Innovation Actions: Proposals may cover one or both 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.
  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).

b. Coordination and Support Actions

To complement the research and innovation activities in this topic as well as topic DS-5-2017: "Secure digital identities for Europe", support and coordination actions should address the following:

- Identify and investigate ethical issues surrounding Privacy, Data Protection and Digital Identities;
- Support the integration of results coming from the various projects related to this topic in order to provide an overall view of the area;
- Support dissemination (including the organisation of an annual domain workshop) and the production of relevant material synthesizing the R&I activities;
- Identify and support liaison with relevant projects in other areas within H2020
- Support the standardisation efforts of the RIAs and coordinate with relevant efforts undertaken by standardisation organisations and technical fora; Identify and propose actions to be included in the European Commission's ICT Standardisation Rolling Plan.
- Contribute to the related areas of the Strategic Research Agenda of the NIS Platform Working Group 3 (WG3) and other related research road-mapping activities;

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.

b. Coordination and Support Actions

Budget per type of instrument(s):

a. Innovation Actions: 19

b. Coordination and Support Actions: 1 MEUR. 1 CSA will be selected.

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), 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)	*€6.500.000,00*	-

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

3 – Evaluations of the proposals for the 2016 and 2017 calls "Disaster-resilience: safeguarding and securing society, including adapting to climate change", "Fight against crime and terrorism" and "Border Security"

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

Type of action: Coordination and Support Action – Expert contracts

Indicative budget:

4 – Evaluations of the proposals for the 2016 and 2017 calls "Digital Security: Cybersecurity, Privacy and Trust"

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 1.00 million from the 2016 and up to EUR 1.00 from the 2017 budget for points a) and b); up to EUR X.XX million from the 2016 and from the 2017 budget for point c)