24.3.2017

EN

Annex 17

Horizon 2020

Work Programme 2018 - 2020 : draft orientations

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

IMPORTANT NOTICE

These draft orientations to prepare the Work Programme 2018-2020 have been elaborated on the basis of the scoping paper 2018-2020.

This document contains elements aimed at facilitating an early discussion with the Programme Committee. It does not represent a draft work programme, and may change in both content and structure, even substantially.

Table of contents

Introduction

Meaning of the "Impact" section:

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

Meaning of the mandatory participation of specific entities:

When a topic has eligibility and admissibility conditions which state: "mandatory participation of" specific entities (e.g.: '3 Law Enforcement Agencies (LEA) from 3 different MS or AC) means that these entities have to be participants and should be directly involved in the carrying out of the tasks foreseen in the grant. See also "Meaning of practitioners".

Meaning of practitioners

A practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants are invited to identify clearly which members of the consortium they consider "practitioners" in the specific context of their proposal, and to include a clear description of their respective role and added-value as practitioners in section 4.3 of proposal part B4-6.

Meaning of "Possible classification":

All topics will be subject to security scrutiny.

Meaning of the "Open Research Data ":

All proposals under this work programme part will be subject to Security Scrutiny. This part of the work programme will not be subject to the Horizon 2020 Open Research Data policy. However individual projects can choose to participate in the Pilot on a voluntary basis. Participating projects will be required to develop a Data Management Plan (DMP), in which they will specify what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. Further guidance on the Pilot on Open Research Data and Data Management is available on the Participant Portal.

Meaning of "Societal aspects":

Security as societal value is a guiding principle throughout this Work Programme. All individual actions must be in compliance with the provisions of the Charter of Fundamental Rights of the European Union.[1]

The applicants must fill in the "Societal Impact Table", as part of the submission process. This table is taken into account during the evaluations under the "Impact" criteria.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

When dealing with the development of technologies, it is recommended that actions consider the concept of "Privacy by Design".

Meaning of Responsible Research and Innovation[2]

The calls under 'Secure societies – Protecting freedom and security of Europe and its citizens' are in line with the Horizon 2020 Responsible Research and Innovation (RRI) cross-cutting issue, engaging society on sensitive security issues, integrating the gender and ethical dimensions, ensuring the access to security research outcomes whenever possible and encouraging formal and informal science education relating to security. Activities will be multi-actor and underpinned by public engagement.

[2] **http://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf**

Boosting the effectiveness of the Security Union - Focus Area

Working to ensure a high level of security for Europeans is an objective set by the Treaties and 'a common European responsibility'. The EU is designed to deliver an area of freedom, security and justice, without internal borders for its citizens. Research efforts are to boost such an endaevor, and coordinate resources from across Horizon 2020 to that effect.It has therefore established a Research and Innovation Focus Area, the aim of which is to support the implementation of the Security Union, reflecting the priorities set out by the Commission. The Focus Area will maximise the synergies among the different parts of Horizon 2020, and deliver concrete solutions for security practitioners in the EU, while at the same time supporting the implementation of the EU policies related to security.

The majority of the Member States depend entirely on Horizon 2020, which represents 50% of the overall public funding for security research in the EU, to cover their needs regarding the development of innovative security solutions. As highlighted by President Juncker in his Political Guidelines: 'Combatting cross-border crime and terrorism is a common European responsibility'.

The focus area aims to achieve:

- **reductions to loss of human life, environmental, economic and material damage from natural and man-made disasters**, including from extreme weather events, industrial accidents, organized crime and terrorism threats, through the development and adoption of innovative solutions.
- **new technologies, solutions and processes for fighting and preventing crime** (including cyber-crime and cyber security), illegal trafficking and terrorism (including cyber-terrorism), and understanding and tackling terrorist ideas and beliefs.
- **research on innovative processes and technologies for action and recovery from post disaster situations**.

Components of the focus area

The Focus Area would span over a broad cross-section of security- and resilience-related topics, from social science investigating how to better cope with violent radicalization, to research and development and innovation in disaster resilience and security missions and operations, in cybersecurity, in communication, observation and detection systems and devices, in dedicated information systems.

- **strengthen the potential impact of security-related research**;
- **better match R&D objectives with security policy needs**;
- **bring security-related research closer to other policies and societal challenges** in the parts of Horizon 2020 where they belong today;

- **jointly contribute to several sets of policy objectives** (e.g. Space policy, Transport policy (also taking into account priorities set in the context of Joint Undertakings/Joint Technology Initiatives), Health policy, Environment policy, Security policy, etc.)

Projects financed as components of the focus area need to be of a sufficient scale to deliver tangible results, and the number of projects kept sufficiently low to be managed by the Commission and the Agency.

Components of the focus area, whose topics are identified as SU-xxx in the Horizon 2020 work programme, include actions from the LEIT-ICT, LEIT-Space and Societal Challenges 1, 6 and 7.

In addition, related activities are financed by other parts of the Horizon 2020 Work Programme including the European Research Council (ERC), the SESAR Joint Undertaking and the ECSEL Joint Undertaking.

Call - Protecting the infrastructure in Europe

H2020-SU-INFRA-2018-2019-2020

Threats against crowded areas and disruptions in the operation of our countries' infrastructure may limit the liberties of our citizens and put at risk the functioning of our societies and their economies. The security and resilience of Europe critical infrastructure needs to be ensured because disruptions in their operations may entail the collapse of large sectors of our activities. Threats on "softer" targets such as crowded areas may have less long-term physical impact, but may be highly damaging due to potentially large numbers of victims and subsequent psychological and sociological impacts.

The topics below in this Call "Protecting the infrastructure in Europe" will be part of the contribution of the Commission to the Cybersecurity contractual Public Private Partnership (cPPP), established in July 2016. This cPPP will facilitate the engagement of end-user operators in sectors that are important beneficiaries and customers of cybersecurity solutions towards defining and providing to the industry their sector-specific digital security, privacy and data protection common requirements.

Mission: The aim is to protect and improve the resilience of critical infrastructures, supply chains and transport modes.

Proposals are invited against the following topic(s):

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

Specific Challenge: Disruptions in the operation of our countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems. Recent events demonstrate the increase of combined physical and cyber-attacks due to their interdependencies. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent installations and systems. Budgetary constraints on both the public and private sectors mean that new security solutions must be more accurate, efficient and cost-effective, and possibly more automated than the ones currently available.

Scope: Proposals should cover: forecast, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs) over the life span of the infrastructure, with a view to achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

They should:

(a) address in detail all aspects of interdependent physical (e.g. bombing, plane or drone overflights and crashes, spreading of fires, floods, seismic activity, space radiations, etc.) and

cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server) and consider the cascading risks of such complex threats

(b) demonstrate the accuracy of their risk assessment approach using specific examples and scenarios of real life and by comparing the results with other risk assessment methodologies and

(c) enhance real-time, evidence-based security management of physical and cyber threats

Innovative methods should be proposed for sharing information with the public in the vicinity of the installations - including through social media and with the involvement of civil society organisations - and the protection of first responders such as rescue teams, security teams and monitoring teams.

In 2018 and 2019, they should focus on any type of installation belonging to one of the following critical infrastructures: water systems, energy infrastructure (power plants and distribution), transport infrastructure, communication infrastructures, health services, e-commerce and the postal infrastructure, and financial services. Priorities for 2020 will be defined at a later stage. When selecting for funding the proposals submitted in 2018 or 2019, the Commission will take due account of similar projects financed further to the INFRA or CIP calls for proposals in the previous years since 2016, with a view to cover the largest possible spectrum of installations.

Consortia should involve the largest variety of relevant beneficiaries, including infrastructure operators, first responders, industry, technologists and social scientists, etc. The participation of SMEs is strongly encouraged.

In line with the EU's strategy for international cooperation in research and innovation [3] international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops with the European Commission. Legal entities established in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 7 – see General Annex G of the Horizon 2020 Work Programme.

[3] COM(2012)497

Indicative budget: The Commission considers that proposals requesting a contribution from the EU of about EUR 8 million would allow this topic to be addressed appropriately. Nonetheless this does not preclude the submission and selection of proposals requesting other amounts

Expected Impact:

Short term:

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.
- Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure.

Medium term

- Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.
- Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure.
- In situ demonstrations of efficient and cost-effective solutions.
- Security risk management plans integrating systemic and both physical and cyber aspects.
- Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.
- Where relevant, test beds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines
- Test results and validation of models of a specific critical infrastructure against physical and cyber threats.
- Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.

Long term

- Convergence of safety and security standards, and the pre-establishment of certification mechanisms.
- Contributions to relevant sectorial frameworks or regulatory initiatives.

Type of Action: Innovation action

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

SU-INFRA02-2019: Security for Smart Cities and "soft" targets in Smart Cities

Specific Challenge: The generation, processing and sharing of large quantities of data is fundamental for the digitisation of cities, aiming to make urban systems and services responsive and able to act upon data in real-time. The distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.

Scope: Screening of the Big Data that is made available in cities - which are being used in part by security practitioners to enhance their capabilities and performances - should be also considered from the perspective of avoiding possible criminal misuse (e.g. digital security measures such as layered authentication and access).

Proposed pilots should address at least one of the following key points:

- Simulation, detection and analysis of the additional security threats and risks created through the interconnection of smart systems (e.g. IoTs, in particular those IoT objects used by security practitioners) and smart infrastructures (e.g. smart (government) buildings, smart railways, smart ports, smart factories, smart bridges, smart hospitals, large gathering of people in smart infrastructure) within a smart city;

- Delivery of a cyber-security framework to ease collaboration across all smart cities stakeholders, from urban planners to infrastructure operators, security practitioners, IT supervisors and providers across smart organizations within the city;

- Support and implementation of a common approach to securing and managing the data from all the smart infrastructures and systems hosted in a smart city supporting the citizens, the public authorities, the security practitioners, and the urban economy in creating transparent, efficient, accountable cyber-secure data-handling processes.

Digital security awareness should be integrated into the eco-system of humans, competences, services and solutions which should be able to adapt rapidly to the evolutions of cyber-threats or even to surpass them.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 7 – see General Annex G of the Horizon 2020 Work Programme

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

Expected Impact:

- Creation of dedicated, harmonised, advance cybersecurity solutions for smart cities adopting common approaches with all involved stakeholders (e.g. administrators of smart city/port/transport) balancing their – sometimes conflicting – goals (e.g. urban development, efficiency, growth, competitiveness, resilience).

- An easier level of integration by developing a holistic cyber-security framework for smart cities that benefits all smart infrastructures hosted within it (e.g. smart buildings, smart ports, smart railways, smart logistics).

- Built IoT ecosystems (rather than distributed IoT infrastructures) adopting common approaches in their cybersecurity management, achieving economies of scale (e.g. avoiding duplication of efforts in the analysis of IoT data, selection of cybersecurity controls).

Type of Action: Innovation action

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

Conditions for the Call - Protecting the infrastructure in Europe

Opening date(s), deadline(s), indicative budget(s):[4]

Topics (Type of Action)	Budgets (EUR million)	Deadlines
Opening: 01 Mar 2018		
SU-INFRA01-2018-2019-2020 (IA) SU-INFRA02-2019 (IA)		
Overall indicative budget		

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and
- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

Eligibility and admissibility conditions: The conditions are described in General Annexes B and C of the work programme.. The following exceptions apply:

SU-INFRA01-2018-2019-2020	At least 3 operators of the chosen type of critical infrastructure operating in 3 Member States or Associated Countries must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of industry able to provide security solutions is required.
SU-INFRA02-2019	At least the local governments of 3 cities or metropolitan areas in 3 Member States or Associated Countries must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement

[4] The budget figures given in this table are rounded to two decimal places.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

	and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of industry able to provide security solutions is required.

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

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Consortium agreement:

	Members of consortium are required to conclude a consortium agreement, in principle prior to the signature of the grant agreement.

Call - Security

H2020-SU-SEC-2018-2019-2020

Disaster-Resilient Societies

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.

Mission: The aim of this section is to reduce the loss of human life a,d to reduce environmental, economic and material damage from natural and man-made disasters, including from extreme weather events, industrial disasters, crime and terrorism threats.

Proposals are invited against the following topic(s):

SU-DRS01-2018-2019-2020: Human factors, and social, societal, and organisational aspects for disaster-resilient societies

Specific Challenge: The resilience of societies heavily depends on how their citizens behave individually or collectively when preparing for, reacting to and overcoming disasters. The spread of new technologies and media are inducing dramatic changes in people's behaviour and are affecting societies in unpredictable ways. Resilience in the future requires a better understanding and implementation of these new technologies and media.

Scope: Proposals are invited to address related research and innovation issues, in particular:

Recent dramatic events either related to natural causes (flash floods, earthquakes, avalanches) or terrorist attacks have alas illustrated that European society is not well prepared to react to disasters. This is largely due to insufficient risk awareness and resilience among the people in Europe, compared to those observed in countries constantly under threat e.g. Japan with risks of earthquakes and tsunamis. Research is required with a view to creating a stronger culture of risks in Europe, including prevention (education, awareness) and preparedness (knowing how to react), emergency management (communication before and during an event) and response (empowering citizens to act by themselves following established guidelines). Diversity in risk perception, in vulnerabilities and in understanding responses to crises requires research that addresses the issues of geographical diversity (within Europe), attitudes, gender and socio-economic contexts, in order to propose new approaches and strategies for community awareness, for leadership, and for crisis readiness and management.

Over the past few years several ways to exploit social media in emergency situations have been studied, and some put in place, the impact of which are not well known. Research is needed to assess such practices for different disaster scenarios (natural hazards, industrial disasters, terrorist threats) involving different actors, including first responders, city authorities and citizens. Research must analyse both the positive and negative roles of social media in crisis situations: in the wake of a terror attack or natural disaster they offer an incredibly quick and

easy way to relieve friends and family from worry; they have been used to spread important safety information. However, social media may also be used to spread false statements and to overstate threats.

For achieving disaster-resilient societies the research community needs appropriately to transfer research outputs to meet citizen expectations given the insufficient awareness and involvement of civil society organisations in a mediating role. Civil society organisations, first responders and city authorities are invited to propose strategies to enable citizens better to access research results related to disaster resilience, and to prepare the ground for exercises involving citizens. These strategies must be tested with citizens representative of European diversity and for different types of disaster, in particular with regards to citizens' individual capacities and their involvement in checking and validating proposed tools, technologies and processes for disaster management. Studies will assess the value of raising awareness about relevant research among citizens.

Proposals should be submitted by consortia involving relevant security practitioners and civil society organisations. Research should contribute to the understanding of society's awareness to risks in Europe in order to provide recommendations for the development of a culture of improved preparedness, adaptability, and resilience to risks, including the use of social media and involving the citizens in the investigations and possible validation of tools and methods.

In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged (but not mandatory), in particular with Japan: Co-funding opportunities from the Japan Science and Technology Agency exist for Japanese partners. For more information, please consult http://www.jst.go.jp/sicp/announce_eujoint_03_GeneralInfo.html. The quality of the international cooperation will be reflected in the evaluation of the proposal, under the criteria 'Excellence' and 'Impact'. Legal entities in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action.

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

Expected Impact: As a result of this action, Member States and Regional authorities as well as City and Metropolitan authorities should benefit from recommendations and tools aimed at improving the adaptability and preparedness of societies to different disaster risks, including:

- Comparative analysis of different approaches to adapt and be prepared to risks in different countries (both within and outside the European Union);
- Identification of existing tools for an improved prevention (including risk understanding and communication), preparedness (including training involving citizens), alert systems

and their recognition by citizens, and responses using citizen's competencies and local knowledge;

- Improved information exchanges among different actors involved, including first responders, local authorities, schools, and citizen representatives;
- Field-validation of different approaches related to different disaster risks involving the above actors, in representative urban environments.

Type of Action: Research and Innovation action

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

SU-DRS02-2018-2019-2020: Technologies for first responders

Specific Challenge: Resilience is critical to allow for authorities to take proper measures in response to severe disasters (natural or manmade). Innovation for disaster-resilient societies may draw from novel technologies, provided that they are affordable, accepted by the citizens, and customized and implemented for the needs of first responders.

Scope: Proposals are invited to address related research and innovation issues, in particular:

- Sub-topic 1: [2018] Victim-detection technologies

The quick detection of victims potentially trapped in buildings as a result of disasters of natural origins (earthquake, avalanche), accidental (explosions), or of a terrorist origin is a major issue for first responders. Novel technologies must enable them to save the time taken to detect victims who are not visible, enabling more efficient and faster rescue operations leading to higher chances of saving lives.

- Sub-topic 2: [2019] Innovation for rapid and accurate pathogens detection

Novel technologies are required by first responders for the rapid and accurate detection of pathogens.

- Sub-topic 3: [2020] Methods and guidelines for pre-hospital life support

Innovative methodologies and guidelines need to be developed for improved pre-hospital life support.

- Sub-topic: [2018-2019-2020] Open

Other technologies for use by first responders may be subject of proposals (for instance: communicating wearables for first responders; situational awareness systems for first responders using UAV and robots, risk anticipation and early warning technologies, etc.) provided that they involve a large number of first responders' organisations (see eligibility and admissibility conditions.)

Any novel technology or methodology under this topic must be tested and validated, not just in laboratories but also in training installations and through in-situ experimental deployment. First responders must be involved in these activities. Proposals should address the participation of first responders in a systematic manner, and propose new methods on how to involve them and to organise their interaction with researchers when developing, testing, and validating technologies and methods.

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

In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged (but not mandatory), in particular with Korean or Japanese research centres. Co-funding opportunities from the Korean MSIP/NRF exist for Korean partners. For more information, please consult http://www.nrf.re.kr/eng/main and http://www.nrf.re.kr/biz/info/notice/view?nts_no=82388&biz_no=116&search_type=ALL&search_keyword=EU&page=. Co-funding opportunities from the Japan Science and Technology Agency exist for Japanese partners. For more information, please consult http://www.jst.go.jp/sicp/announce_eujoint_03_GeneralInfo.html. The quality of the international cooperation will be reflected in the evaluation of the proposal, under the criteria 'Excellence' and 'Impact'. Legal entities in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: As a result of this action, first responders should benefit from:

- Novel tools, technologies and methods aimed at facilitating their operations in case of disasters or health outbreaks by pathogens, so that lives may be saved by faster and well-targeted rescue operations
- Novel, duly validated detection methods

- Novel methodologies and guidelines for pre-hospital life support for improved triage of victims
- New knowledge about field-validation of different tools, technologies and approaches involving first responders in (real-life) scenarios

Type of Action: Research and Innovation action

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

SU-DRS03-2018-2019-2020: Pre-normative research and demonstration for disaster-resilient societies

Specific Challenge: A reason for the difficult interaction among practitioners, and for the low levels of interoperability of equipment and procedures implemented by first responders, lies in there being insufficient harmonisation and standardisation, which pre-normative research and demonstrations may address effectively.

The security market in Europe is an institutional market highly fragmented (because of the lack of standardization and harmonised certification), with a strong societal dimension (it directly affects in many ways the citizens). In this context, the Mandate M/487 to Establish Security Standards coordinated by the European Committee for Standardization has clearly recognized the crisis management and civil protection as one of the three priorities for establishing standards in the security sector. It has identified the need for crisis management and civil protection standardization activities to facilitate response, effectiveness, efficiency and cooperation as top priorities, especially in what regards to natural hazard emergencies.

Scope: Proposals are invited to address issues related to pre-standarisation, in particular:

- Sub-topic 1: Pre-standardisation for the security of water supply

For several years research actions have led to the development of detection technologies to analyse drinking water. Based on the legacy of FP7-funded actions, clearer strategies to integrate current technologies in the existing water safety network must be designed. Testing facilities must interconnect the safety- and security-related networks of sensors that are deployed among water supply and distribution networks. The focus of action should be on networking testing facilities developed by water utilities to demonstrate the use of current sensor technologies for the purpose of both safety and security of water.

- Sub-topic 2: Methodical demonstration of novel concepts for the management of pandemic crises

In 2014 an exploratory phase was called for (in DRS4) to address the feasibility of strengthening capacity-building for health and security protection in case of large-scale pandemics (phase 1). The resulting PANDEM project has issued a range of recommendations for research gaps to be addressed in priority. It has also proposed innovative concepts to integrate better existing tools

and systems for health and security protection in case of large-scale pandemics. Demonstrations are now required to assess these novel concepts, in support of cross-border emergency approaches (phase 2).

- Sub-topic 3: Pre-standardisation in CBRN-E crisis management

Generally speaking, the development of standards for civil protection in the areas of CBRN-E and crisis management (including for CBRN-E systems, tools and services) will increase interoperability of equipment and procedures. Innovation actions must be taken to bring validated and positively-assessed practices into standards within, or outside current standardisation processes. The involvement of well-established standardisation organisations is required. Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account

- Sub-topic 4: First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means

Improved standards are required for an effective deployment of resources during the advent of a major crisis, when there are strong cross-sector, cross-border, cross-hierarchy coordination activities ongoing. Proposals under this sub-topic should pave the way to such improved standards.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 6 to 7 – see General Annex G of the Horizon 2020 Work Programme.

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

Expected Impact: Medium term:

- full awareness of water supply facilities about the necessity of designing monitoring networks capable of detecting both contamination risks (safety) and deliberate poisoning (security);

- demonstrated novel concepts for health and security protection in the case of large-scale pandemics integrating tools and systems in support to cross-border emergency management:

- standards for interoperable equipment and procedures in the CBRN-E and crisis management areas in support to operations involving international crews.

Type of Action: Innovation action

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

SU-DRS04-2019-2020: Chemical, biological, radiological and nuclear (CBRN) cluster

Specific Challenge: Technologies and innovations in the field of CBRN are developed by companies which often face difficulties in bringing them to markets. At least three reasons may be identified:

- they address local, small niche markets;
- these companies have neither the capabilities nor the strategic objective to go for foreign markets;
- the individual technologies that they develop can make it to the market only if integrated and combined with other tools by other companies that have the capabilities and the strategy to market products abroad, and possibly on the global market.

In this context a platform has been established further to the response to topic SEC-05-DRS-2016-2017 in 2016. A larger number of innovative technologies, devices and services need to be added to this platform.

Scope: In 2019 and 2020 the Commission will select several RIAs aiming at research and development of novel CBRN technologies and innovations identified in the catalogue that is updated by the ENCIRCLE project on a regular basis. Each of these actions will be led by an SME. Each consortium implementing such a RIA must not only establish a consortium agreement among its members, but also an agreement with the participants in the ENCIRCLE project which must settle how the results from the RIA will be exploited and integrated into platforms managed by ENCIRCLE.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 8 – see General Annex G of the Horizon 2020 Work Programme.

Indicative budget: The Commission considers that proposals requesting a contribution from the EU of about EUR 3.5 million per action for this topic to be addressed appropriately. Nonetheless this does not preclude submission and selection of proposals requesting other amounts.

The following options of the Model Grant Agreement will be implemented:

- Option 1 of Article 41.3 of the Model Grant Agreement will be applied.

- *Grants awarded under* this topic *will be complementary to the grant agreement under* **SEC-05-DRS-05-2016-2017 part a)**. *The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement*[5] *will be applied.*

Expected Impact:

- Shorter time to market for novel CBRN technologies and innovations
- More business deals leading to industrial products of interest to more practitioners in Europe (and world-wide).

Type of Action: Research and Innovation action

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

Fight Against Crime and Terrorism

Mission: The ambition of the activities under "Fight against Crime and Terrorism" is to mitigate potential consequences of crime- and/or terrorism-related incidents or to avoid them. To this end, new technologies and capabilities are required. They should address the fight against and the prevention of crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism), along with understanding and tackling terrorist ideas and beliefs. Human factors and the societal context should be taken into account, whilst respecting human rights and privacy.

Proposals are invited against the following topic(s):

SU-FCT01-2018-2019-2020: Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism

Specific Challenge: The free and democratic EU society, based on the rule of law, mobility across national borders, globalized communication and finance infrastructure provide many opportunities to the people. However, they come along with by risks related to crime and terrorism, a significant number of which cross-border impacts within the EU. Security is a key factor to ensure a high quality of life and to protect our infrastructure through preventing and tackling common threats. The EU must prevent, investigate and/or mitigate the impact of criminal acts, whilst protecting the fundamental rights of citizens. The consistent efforts made by EU Member States and the EU to that effect are not enough, especially when criminal groups and their activities extend far beyond national borders.

Scope: The Lisbon Treaty enables the EU to act to develop itself as an area of freedom, security and justice. The EU Security Union is now in the building, and requires an EU-wide approach

[5] *http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf*

to security that integrates prevention, investigation and mitigation capabilities in the area of the fight against crime.

The globalisation of communications and finance infrastructure allows for crime to develop and take new forms. Trafficking in human beings for all forms of exploitation purposes is a serious and organised crime often with cross-border dimension, violating fundamental rights of the individuals and creating a security challenge. Prevention of child sexual abuse and exploitation is another area where research is acutely needed. The use of the internet as a platform for child sex offenders to communicate, store and share child sexual exploitation material and to hunt for new victims continues to be one of the internet's most abhorrent aspects. Cybercriminality, as a whole, is not satisfactorily understood nor properly addressed; the constantly expanding attack surface combined with the ever increasing number of attack vectors requires a more structured approach. Radicalisation is yet another challenge of our society that requires a multi-disciplinary approach, with policy recommendations and practical solutions to be implemented by a variety of policy-makers and practitioners.

Proposed approaches need to rely on existing knowledge and exclude prior failed approaches. The societal dimension of fight against crime and terrorism must be at the core of the proposed activities. Proposals should be submitted by consortia involving relevant security practitioners and civil society organisations, each under only one of the following sub-topics:

- Sub-topic 1: [2018] New methods to prevent, investigate and mitigate trafficking of human beings

Preventing the phenomenon and reducing the demand for all forms of exploitation in the trafficking chain (legal and illegal sectors) are important aspects of preventing this crime. Analysis of possible involvement of organized crime groups implicated in trafficking of human beings in other crimes as well (e.g., money laundering, smuggling) is encouraged.

- Sub-topic 2: [2018] New methods to prevent, investigate and mitigate child sexual exploitation

Peer-to-peer networks and the growing number of forums on the Darknet continue to facilitate the exchange of child sexual exploitation material and support offenders. Further research is required to address these developments and provide law enforcement with effective means to prevent and investigate this type of crime.

- Sub-topic 3: [2019] Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour

The Internet of Things (IoT), ever increasing number of internet-facing devices, may pose substantial threats to (cyber) security, as it has become a target for cybercriminals. The key challenge with this respect is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated.

- Sub-topic 4: [2020] Developing comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation in the EU

Of particular interest: how to address returnees, with a special focus on children and women, and how they relate to petty crime; resurgence of lone actor phenomenon: gender aspects of radicalisation; counter-narratives and alternative narratives; polarisation in society and the shift from risk factors to resilience factors. Proposals should refer to research that compared various approaches to these issues, and build on the assessment and evaluation of current and past counter and de- radicalisation initiatives. In line with the EU's strategy for international cooperation in research and innovation, international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops with the European Commission. Legal entities established in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action.

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other way to solve issues in fighting against crime and terrorism, and supported by large numbers of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

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

Expected Impact: Medium term:

- improved and consolidated knowledge among EU Law Enforcement Agencies officers on the issues addressed in this topic
- exchange of experiences among the EU Law Enforcement Agencies (LEAs) about human, social and societal aspects of security problems and their remedies;
- policy-making toolkits for security policy-makers, to support the establishment of a European Security Model;
- toolkits for LEAs and/or civil society organisations, validated against practitioners' needs and requirements to facilitate their daily operations;

Long term:

- European common approaches for assessing risks/threats, and identifying and deploying relevant security measures, which take into account legal and ethical rules of operation as well as cost-benefit considerations.

- Support towards the implementation of the European Security Union by strengthening the perception by citizens of the EU as an area of freedom, justice and security.

Type of Action: Research and Innovation action

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

SU-FCT02-2018-2019-2020: Technologies to enhance the fight against crime and terrorism

Specific Challenge: Organized crime and terrorist organisations are often at the forefront of technological innovation in planning, executing and concealing their criminal activities and the revenues stemming from them. Law Enforcement Agencies (LEAs) are often lagging behind when tackling criminal activities supported by advanced technologies.

Scope: There is a growing need to focus on technology opportunities provided by new and emerging technologies. To this end, it is necessary to identify new knowledge and targeted technologies for fighting both old and new forms of criminal and terrorist behaviour supported by advanced technologies. Challenges are numerous. In conventional investigations, rapid and near real-time forensics is often crucial for preventing subsequent attacks or crimes. A consequence of the increasing digitisation of society and ever increasing adoption levels is that virtually any type of crime has a digital forensics component, which is a challenge in itself. Money-flow tracking represents yet another challenge. The issues of location and jurisdiction need to be addressed, taking into account highly probable cross-border nature of such crimes.

Proposals should be submitted under only one of the following sub-topics:

- Sub-topic 1: [2019] Trace qualification

Forensic analysis of trace material can be extremely helpful in the initial phase of investigation, if the answers are rapid (near real-time), at an acceptable cost and compliant with criminal justice. There is a need for a better knowledge and interpretation of: trace composition, time when they were left, cause of their origin (crime-related or inoffensive), etc.

- Sub-topic 2: [2018] Digital forensics in the context of criminal investigations

New forensic tools and methodologies are needed, based on common practices, standards, protocols and/or interoperability requirements that allow for rapid retrieval, storage, analysis and validation of digital evidence (including the one stored in the cloud) that upholds in court. They should focus on data exploitation, and speedy exchange of information. All types of crime, terrorist activities, and malicious acts by foreign-state perpetrators are concerned. Research in

this domain should take into account new and emerging trends (for instance, use of encryption), while fully respecting fundamental rights and privacy.

- Sub-topic 3: [2020] Money flows tracking

Organized crime increasingly uses internet/Darknet as a facilitator for preparation, organisation and execution of various physical/traditional criminal activities (e.g., child sexual abuse, trafficking of human beings, trafficking of firearms, terrorism) and/or as a tool for online criminal activities (e.g., ransomware, domain-name piracy, phishing). Here, research should address: approaches to identify changing tracks (new markets and networks); tools for tracing money-flow/criminals online whilst protecting personal privacy; Darknet marketplace analysis and mobility; tools for locating and mapping hidden service directories; data provenance models (providing court-proof evidence).

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge (for instance: technologies to improve LEAs capabilities (including augmented reality); autonomous systems to improve the fight against crime and terrorism; technologies to support better protection of public figures) and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

In all sub-topics and in order to facilitate the EU-wide take-up of new technologies, proposers are encouraged to include the design of innovative curricula for LEAs training and (joint) exercises, and of information packages for the wider public and civil society organisations.

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- novel, user-friendly technologies, tools and/or systems, addressing traditional or emerging forms of crime and terrorism at acceptable costs;
- improved investigation capabilities, especially regarding quality and speed;
- increased efficiency and effectiveness of the information sharing among EU LEAs;

Long term:

- prevention/reduction of criminal and terrorist threats;
- harmonisation of information formats at international level, improved cross-border acceptance and exchange of court-proof evidence, standardised evidence collection and harmonised procedures in the investigation of trans-border crimes.

Type of Action: Research and Innovation action

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

SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism

Specific Challenge: Large amounts of data and information from a variety of origins have become available to practitioners involved in fighting crime and terrorism. Full advantage is not currently taken of the most advanced techniques for Big Data analysis, and artificial intelligence.

Scope: The amount of data generated and gathered in the frame of (cyber)crime investigations increases exponentially, thereby creating a considerable challenge for law enforcement. The effectiveness of law enforcement action depends on the capability to convert voluminous and heterogeneous data sets (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) into actionable intelligence. They could be enhanced in a significant manner by the use of domain-specific tools, i.e. big data analysis applications designed for the needs of crime investigators (pre-processing, processing and analysis, visualisation, etc.). Furthermore, predictive analytics would greatly benefit from open source intelligence gathering, and social network data analysis, and allow for resource-efficient, effective and proactive law enforcement.

The internet of things connects practically everything and makes everything more vulnerable as well. Wearable devices make us traceable, 3D printers can produce weapons, autonomous cars provide opportunities for kidnappers, teleworking opens doors for cyber-espionage etc. Cybercriminals follow the technological development and benefit from it, while measures for countering cybercrime are often one step behind. LEAs would benefit from new means of preventing and countering new kinds of crime, building on the comprehensive trend analysis of emerging cybercrime activities based on past of (cyber)criminal activities, on technological developments, and on trends in the society.

Criminal and terrorist acts are usually subsequent to abnormal behaviours. Behavioural/anomaly detection systems (using a large variety of sensors) and methodologies require the analysis and processing of enormous quantities of data, together with improved imaging. Such systems should operate in near real-time and at similar distances as a surveillance camera. They should also comply with privacy requirements and the respect of fundamental rights.

Proposals are invited from consortia involving relevant security practitioners, civil society organisations, and the appropriate balance of IT specialists, psychologists, sociologists, linguists, etc. exploiting big data and predictive analytics: a) to caracterize trends in cybercrime and in cybercriminal organizations (based on a profound analysis of current and emerging cybercriminal organizational types and structures), and b) to enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (shopping malls, entertainment venues, etc.).

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 5 to 7 – see General Annex G of the Horizon 2020 Work Programme.

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

Expected Impact: Medium term:

- improved support for the work of LEAs in managing big data, i.e. in extracting, combining, analysing and visualising large amounts of structured and unstructured data in the context of criminal investigations;
- increased awareness regarding the state of the art and trends in cybercriminal activities (short-, mid- and long-term);
- in-depth knowledge of means of preventing and countering emerging and future cybercriminal activities;
- shorter delays between the emergence of new cybercrime activities and the deployment of countermeasures;

Long term:

- a European, common strategic approach for preventing and countering an emerging cybercrime activity in its early stage of development;
- a European, common strategic approach for processing and combining huge amount of data in the context of crowd protection.

Type of Action: Innovation action

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

SU-FCT04-2020: Explosives: detection, intelligence, forensics

Specific Challenge: Explosives remain a major threat in the hands of wrongdoers. The nature of explosives change over time and their manufacturing methods evolve continuously, which makes the specialized work of law enforcement agencies (LEAs) in this area a continuous challenge.

Scope: To be defined in 2019.

The Commission considers that proposals requesting a contribution from the EU of about EUR 10 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Type of Action: Research and Innovation action

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

Border and External Security

This section concerns strengthening security through border management. This includes both control and surveillance issues. It contributes to the further development of the European Border Surveillance System (EUROSUR) and promoting an enhanced use of new technology for border checks, also in relation to the Smart Borders legislative initiative. It also addresses supply chain security in the context of the EU's customs policy.

Mission: The aim is to develop technologies and capabilities which are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security, whilst respecting human rights and privacy. New technologies, capabilities and solutions are also 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 also 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.

Proposals are invited against the following topic(s):

SU-BES01-2018-2019-2020: Human factors, and social, societal, and organisational aspects of border and external security

Specific Challenge: Border and external security may depend on a variety of human factors, and social and societal issues, and on the adoption of appropriate organisational measures, which are all deeply influenced by the advent of novel technologies and social media, in ways which are not well understood, but that need to be. One main challenge is to manage the flow of travellers and goods arriving at our external borders, while at the same time tackling irregular migration and enhancing our internal security. Any novel technology or organisational measure will need to be accepted by the European citizens.

Scope: Proposals are invited to address related research and innovation issues, each under only one of the following sub-topics:

- Sub-topic 1: [2018] Detecting security threats resulting from misperceptions about the EU

Better detecting and understanding how the EU is perceived in countries abroad by analysing social media data, and designing counter-arguments when the perception of the EU is leading to threats on its citizens and territories - in order for instance to counteract tendencies and correct skewed images of Europe. Proposals should investigate which solutions to bring to such issues. In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged. The quality of the international cooperation will be reflected in the evaluation of the proposal, under the criteria 'Excellence' and 'Impact'. Legal entities in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action.

- Sub-topic 2: [2019] Modelling, predicting, and dealing with migration flows to avoid tensions and violence

Better modelling and predicting migration flows, based on a sound analysis, is required for high level strategic decision-making, for planning and implementing operational activities. For the management of the migratory flow, including relocations within the EU, it is necessary to map public sentiment, including perceptions of migration, by analysing data available from many different governmental or public sources, and by developing socio-economic indicators of integration strategies. Proposals should be solution-oriented and address how to better deal with such flows and to reduce risks of tensions and violence among migrants and European citizens.

- Sub-topic 3: [2020] Developing indicators of threats at the EU external borders on the basis of sound risk assessment methodologies

Threat factors at the EU external borders range from uncontrolled, massive flows of people arriving at the borders to the use of counterfeit documents. Proposals need to develop indicators that would assess the risks at the border to contribute to the effectiveness of border control. Proposals should consider that for some risks indicators will build upon large volumes of underlying data in many formats (detections of illegal border-crossing), while for others they will deal with very small volumes (detections of document fraud). The proposed research should also take account of the newly developed Vulnerability Assessment Methodology that foresees setting up a system of continuous scanning and annual baseline assessments. Proposals should be solution-oriented, and develop indicators helpful to relate external and internal security factors.

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

Proposals should pursue truly innovative approaches. They should be submitted by consortia involving relevant security practitioners and civil society organisations. Synergies are encouraged with the work for the knowledge centre and demography set up by the Commission https://ec.europa.eu/jrc/en/migration-and-demography.

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

Expected Impact:

- Knowledge and evidence-based support to policy developments, validated by policy-makers and practitioners in the Member States.
- Methods to better manage the complexity (from reducing the incentives for irregular migration, to the analysis and sharing of best practices, and towards an effective application of common rules…) of the issues addressed in this challenge, validated by practitioners and civil-society organisations.

Type of Action: Research and Innovation action

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

SU-BES02-2018-2019-2020: Technologies to enhance border and external security

Specific Challenge: Innovation for border and external security may draw, in particular, from novel technologies, provided that they are affordable, accepted by citizens and customized and implemented for the needs of security practitioners.

Scope: Proposals are invited to address related research and innovation issues, in particular:

- Sub-topic 1: [2018] Providing situational awareness and applying augmented reality to border security

Currently, information is made available to border guards in several formats and on different kinds of displays. However, human cognitive is limited to managing information from several sources simultaneously and to handling too many separate pieces of equipment is limiting

ability to act. Furthermore, border guards often work in sparsely populated and remote areas where the availability of telecommunication networks may be an issue. Research and innovation must lead towards (cloud-based) systems with simple but complete interfaces showing real-time information in the actual context of operation, in a user-friendly way, and assisting border guards in decision-making, whilst remaining in contact with their command and control centre.

- Sub-topic 2: [2018] Detecting fraud, verifying document validity, and alternative technologies to identifying people

The use of counterfeit travel documents at borders is a reality, which entails the risk of not identifying known criminals, including terrorists. New countermeasures are needed to address potential frauds, in particular for the detection of morphed face images, and using for instance biometrics "on the fly" techniques (without interrupting the flow of people in a non-intrusive manner).

- Sub-topic 3: [2019] Security on-board passenger ships

Security on-board passenger ships is challenging, given the larger number of specific constraints that apply. Technologies are needed, as well as methods for their deployment, to ensure security all along the "life cycle" of a voyage.

- Sub-topic 4: [2020] Disruptive sensor technologies for border surveillance

Sensor technologies are critical in the context of border surveillance, including novel radar technologies, multispectral sensors, lidar sensors, acoustic sensors, electronic support measures, etc. as well as their miniaturization, integration fusion, and cross-cueing under extreme atmospheric conditions.

- Sub-topic 5: [2019] Detecting threats in the stream of commerce without disrupting business

The flow of goods crossing borders is increasing, whilst ways of concealing methods for dangerous materials and illegally trafficked goods are improving. The detection of such dangerous and illegal goods must be facilitated by novel technologies and sensing strategies that can be implemented without disrupting business.

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Clear, realistic benchmarks against which to assess progress, so as to possibly stop the project if at mid-term review
- Plan to provide confidence in the take up of project results after the completion of the project

Medium term:

- Evidence based knowledge, and developments performing beyond the current state of the art and leading quickly to innovation
- Technical and operational guidelines, recommendations and best practices set in the Eurosur Handbook

Long term:

- Implementation of solutions resulting from the legislative initiative in the "Smart Borders" package
- Implementation of actions of civilian nature identified in the EU Maritime Security Strategy action plan

Type of Action: Research and Innovation action

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

SU-BES03-2018-2019-2020: Demonstration of applied solutions to enhance border and external security[6]

Specific Challenge: Solutions at high Technological Readiness Levels (TRL; please see Annex G of the General Annexes) exist to enhance border and external security, but they need to be demonstrated in the context of actual operations or exercise for validation by practitioners, or to remain unused.

[6] This activity directly aimed at supporting pilot activities is excluded from the delegation to the Research Executive Agency and will be implemented vy the European Border and Coast Guarg Agency

Scope: Consortia are invited to propose demonstration of high (6-8) Technology Readiness Levels (TRL) systems applied in the context of border and external security. (TRL: please see Annex G of the General Annexes.)

Proposals should be submitted under only one of the following sub-topics:

- Sub-topic 1: [2019] New concepts for decision support and information systems

Information systems to support border and external security may combine a broad variety of data from very different sources. Innovative solutions are needed to ensure the availability of information for maritime border surveillance coming from the area of operations, when and where it is needed, thus at enhancing situation awareness at strategic level (in National Coordination Centres), but also at tactical level (with assets deployed under the frame of surveillance operations). This would allow faster reaction and a reduction in the death toll at sea. Proposals should aim at optimize the exploitation of data for their specific use in surveillance is currently embryonic, and needs to take better account of the specific characteristics of the domain, with a view to provide the needed information reducing redundancies.

- Sub-topic 2: [2020] Improved systems for the detection, identification and tracking of small boats

The detection, identification and tracking of small boats is quite challenging since systems need to cover large maritime areas, large numbers of small boats, limited performance of radars and cameras, and the limited possibility to separate those small boats travelling from one Schengen country to another, from those travelling from or to outside a Schengen country. Proposals should aim at innovative solutions to improve border surveillance at sea, to enhance situation awareness in (national) command and control centres, to track the boats' destinations, and to detect possible illegal activities or to provide for search and rescue.

- Sub-topic 3: [2018] Remotely piloted aircrafts and underwater autonomous platforms to be used from on-board offshore patrol vessels

Remotely piloted (aircraft and underwater) autonomous platforms, must demonstrate innovative capacities for border surveillance in the pre-operational environment also in connection with high-altitude and satellite platforms. Research on artificial intelligence is likely to facilitate the transition from innovation to operation. Such platforms play an important role in facilitating long range and persistent surveillance in large maritime areas, complementing operation from offshore patrol vessels. Improving the cost effectiveness, reliability and availability of such platforms, either by increasing the performance of existing technologies or by developing innovative concepts of operation, would notably contribute to a better situational awareness at the tactical level beyond coastal waters (up to 200 nautical miles), while reducing risks during search and rescue missions. Proposals should aim at improved cost effectiveness, in particular through the remote operation of sensors mounted on aerial platforms (including

optionally and remotely piloted) and by improving the on-board processing of payload data, while minimizing the data transmission to the ground segment.

- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals submitted under this topic should be coordinated by a practitioner organization under civilian authority and command. They should clearly demonstrate how they complement and do not overlap with actions undertaken in the Preparatory Action on Defence Research under topic *PADR-US-01-2017: Technological demonstrator for enhanced situational awareness in a naval environment.*

Certain operational costs are excluded from eligible costs (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, including privacy and fundamental rights.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- Innovative solutions validated and qualified in the real, operational environment of civilian missions, defined in detail according to specifications set by the practitioners (authorities in charge of border surveillance) and tailored to effectively meet their requirements within civilian missions.
- Plans for the quick take up of qualified systems at EU level.
- Plans for transnational procurement strategies.

Long term:

- Improved cost-effectiveness and efficiency of systems for the prevention of cross border crime and for border surveillance for civilian purposes.
- Substantial and tangible improvement of situational awareness and reaction capability, as appropriate in border surveillance for civilian purposes, fight against crime and search and rescue missions by the National and European Border and Coast Guards.
- Contribution to the concept of Common Application of Surveillance Tools, as for the European Border Surveillance System (EUROSUR)

Type of Action: Innovation action

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

General Matters

Proposals are invited against the following topic(s):

SU-GM01-2018-2019-2020: Pan-European networks of practitioners and other actors in the field of security[7]

Specific Challenge: In Europe, practitioners interested in the uptake of security research and innovation are dedicated to performing their duty and are focused on their tasks. In general, however, practitioner organisations have little scope to free workforces from daily operations in order to allocate time and resources to monitor innovation and research that could be useful to them. They have few opportunities to interact with academia or with industry on such issues. All stakeholders – public services, industry, academia – including those who participate in the Security Advisory Group, recognize this as an issue.

Scope: Practitioners are invited to associate in 4 different categories of networks in the field security:

a. [2019-2020] Practitioners (end-users) **in the same discipline and from across Europe** are invited to get together: 1) to monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results, 2) to express common requirements as regards innovations that could fill capability and other gaps and improve their future performance, and 3) to indicate priorities as regards areas requiring more standardisation. Proposals are invited in areas of specialisation, for instance but not exclusively: protection of public figures; forest firefighting; forensic police; etc.

b. **[2018] Innovation clusters from around Europe** (established at national, regional or local level), especially those managing **demonstration sites, testing workbenches, and training facilities** (including those providing simulators, serious gaming platforms, testing of PPDR applications on broadband networks) are invited to establish one network 1) to establish and maintain a roster of capabilities and facilities, 2) to organise to share expertise, 3) plan to pool and share resources with a view to facilitating access to their respective facilities among collective membership when this would constitute an economy of scale and allow a more intensive use of expensive equipment, and 4) to coordinate future developments and workbenches' acquisition.

c. [2018] Procurement agencies, or departments, active at budgeting and implementing the acquisition of security solutions at European, national, regional or local level can get together:

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

1) to share investment plans, 2) to compare procurement techniques and rules, and 3) to plan for common procurements of research services as well as of innovative, off-the-shelf products**.**

d. [2018] Border and coast guard organisations, procurement authorities, industry and researchers are invited to join forces and draft the roadmaps necessary to provide innovative solutions for border surveillance, control and management. Whilst practitioners must clearly be in the lead for expressing requirements, the largest number of (national) research organisations and industry participants must be involved in the consortium. The management of EU borders requires more interoperability among systems in order to improve capabilities. Industry is not encouraged to invest in innovation given the small size of national markets and national authorities hesitate to invest in innovative solutions not knowing the intentions of their neighbours and of other countries. A roadmap is required for border and coast guard authorities, and industry, to plan ahead and to facilitate future investments into common, interoperable solutions and systems. Border and coast guards organisations, procurement authorities, industry and researchers are invited to join forces and draft the roadmaps necessary to provide innovative solutions for border surveillance, control and management. Whilst practitioners must be in the lead for expressing requirements, the largest number of (national) research organisations and industry participants must be involved in the consortium.

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.

The Commission considers that proposals requesting a contribution from the EU of:

- about EUR 3.5 million per action for a duration of 5 years (recommended duration) for Parts a), b) and d);
- about EUR 1.5 million per action for a duration of 5 years (recommended duration) for Part c)

would allow for this topic to be addressed appropriately. Nonetheless this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- Common understanding of innovation potential, more widely accepted understanding, expression of common innovation and standardization needs among practitioners in the same discipline.
- Greater involvement from public procurement bodies upstream in teh innovation cycle.
- More efficient use of investments made across Europe in demonstration, testing, and training facilities.

Long term:

- Synergies with already established European, national and sub-national networks of practitioners, even if these networks are for the time being only dedicated to aspects of practitioners' work unrelated to research and innovation (in general, to the coordination of their operations).

Type of Action: Coordination and support action

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

SU-GM02-2018: Common requirements specifications for innovative, advanced systems to support security[8]

Specific Challenge: Innovative solutions must support the European Union when national resources are required to work more closely together when engaged in border and external actions.

Scope: Practitioners from several countries are invited to work on common requirements of any kind of system that they may need in the future to enhance border and external security, to fight against crime and terrorism, to protect infrastructure, or to make societies more resilient, and to involve their respective procurement bodies in preparing for future acquisitions.

To ensure that the outcome of this action becomes also available to EU Member State national authorities as well as EU agencies not participating for further procurement purposes, proposals must necessarily state:

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

(2). Commitment from participating procurement authorities to consult with any legal entity generating information to be released for the purpose set out in paragraph (1), unless contrary to applicable legislation.

(3). Commitment from participating procurement authorities to negotiate the use granted under paragraph (1) on Fair Reasonable and Non-Discriminatory (FRAND) terms.

The following options of the Model Grant Agreement will be implemented:

- Options on additional exploitation obligations of Article 28.1 of the Model Grant Agreement will be applied.

[8] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies and supporting various groups of stakeholders, and public-public partnerships with Member States and associated countries is excluded from the delegation to the Research Executive Agency and will be implemented by the Commission services.

- *Grants awarded under* this topic *will be complementary to the grant agreement under* **SU-GM03-2020**. *The respective options of Article 2, and Article 41.4 of the Model Grant Agreement*[9] *will be applied.*

A subset of the domains addressed by the proposals selected for funding by the Commission will be continued with pre-commercial procurement activities in 2020.

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

The Commission considers that proposals requesting a contribution from the EU of about EUR 1 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Common requirements for innovative prototypes agreed among the practitioner organisations involved in the action
- Technical tender documents ready for use by subsequent pre-commercial procurement actions, as well as by non-participating procurement authorities

Drafting Comment: Type of Action: CSA

Type of Action: Coordination and support action

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

SU-GM03-2020: Pre-commercial procurements of innovative, advanced systems to support security

Specific Challenge: Innovative, research-based solutions must support the European Union when its national resources are required to work more closely together when engaged in actions to improve security.

Scope: Practitioners from several countries are invited to proceed with pre-commercial procurements based on common requirements resulting from activities financed under SU-GM02-2018, which will be made available on due time.

Phase 1: To finalise the tenders packages for calls for tenders to build security-relevant prototypes based on the technical input to tender packages resulting from SU-GM02-2018. To establish methods suitable for the validation of these prototypes across Europe;

[9] *http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf*

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

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

Phase 4: To draft a curriculum for pan European training in using the prototypes.

To ensure that the outcome of this action becomes also available to EU Member State national authorities as well as EU agencies not participating for further procurement purposes, the proposal must necessarily state:

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

(2). Commitment from participating procurement authorities to consult with any legal entity generating information to be released for the purpose set out in paragraph (1), unless contrary to applicable legislation.

(3). Commitment from participating procurement authorities to negotiate the use granted under paragraph (1) on Fair Reasonable and Non-Discriminatory (FRAND) terms.

The following options of the Model Grant Agreement will be implemented:

- Options on additional exploitation obligations of Article 28.1 of the Model Grant Agreement will be applied.
- *Grants awarded under* this topic *will be complementary to a grant agreement under* **SU-GM02-2018**. *The respective options of Article 2, and Article 41.4 of the Model Grant Agreement*[10] *will be applied*.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 8 – see General Annex G of the Horizon 2020 Work Programme.

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

The Commission considers that proposals requesting a contribution from the EU of between EUR 4 to 12 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

[10] *http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf*

Expected Impact: Mid term:

- Pre-commercial prototypes matching requirements common to many Member States, and available from 2 different sources for further industrialisation.

Type of Action: Pre-Commercial Procurement

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

SU-GM04-2018-2019-2020: Pre-commercial procurements of innovative solutions to enhance security

Specific Challenge: Innovative solutions must support the European Union when its national resources are required to work more closely together when engaged in actions to improve security.

Scope: Practitioners from several countries are invited to proceed with the procurement of innovative solutions to enhance their operational capability.

Phase 0: To draft common requirements for innovative prototypes, agreed among the practitioner organisations involved in the action, and to prepare the technical tender documents ready for use in the subsequent phase of the action;

Phase 1: To prepare a full tenders package for calls for tenders to build security-relevant prototypes based on the technical input resulting from Phase 0; to prepare for the validation of the future prototypes;

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

Phase 3: To benchmark and validate the 2 prototypes against the method developed during Phase 1;

Phase 4: To draft a curriculum for pan European training in using the prototypes.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 8 – see General Annex G of the Horizon 2020 Work Programme.

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

The Commission considers that proposals requesting a contribution from the EU of between EUR 2 to 12 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Pre-commercial prototypes matching requirements common to many Member States, and available from 2 different sources for further industrialisation.

Type of Action: Pre-Commercial Procurement

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

Conditions for the Call - Security

Opening date(s), deadline(s), indicative budget(s):[11]

Topics (Type of Action)	Budgets (EUR million)	Deadlines
Opening: 01 Mar 2018		
SU-BES01-2018-2019-2020 (RIA) SU-BES02-2018-2019-2020 (RIA) SU-BES03-2018-2019-2020 (IA) SU-DRS01-2018-2019-2020 (RIA) SU-DRS02-2018-2019-2020 (RIA) SU-DRS03-2018-2019-2020 (IA) SU-DRS04-2019-2020 (RIA) SU-FCT01-2018-2019-2020 (RIA) SU-FCT02-2018-2019-2020 (RIA) SU-FCT03-2018-2019-2020 (IA) SU-FCT04-2020 (RIA) SU-GM01-2018-2019-2020 (CSA) SU-GM02-2018 (CSA) SU-GM03-2020 (PCP) SU-GM04-2018-2019-2020 (PCP)		
Overall indicative budget		

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and

[11] The budget figures given in this table are rounded to two decimal places.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

Exceptional funding rates:

SU-BES03-2018-2019-2020	Cost of fuel is excluded from the costs eligible under the grant agreements implementing this topic.
SU-GM03-2020	The funding rate for actions under this topic is limited to 90% of the total eligible costs.
SU-GM04-2018-2019-2020	The funding rate for actions under this topic is limited to 80% of the total eligible costs.

Eligibility and admissibility conditions: The conditions are described in General Annexes B and C of the work programme.. The following exceptions apply:

SU-DRS01-2018-2019-2020	This topic requires the active involvement of at least 3 first responders' organisations or agencies from at least 3 different EU or Associated countries.
SU-DRS02-2018-2019-2020, SU-DRS03-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 agencies or first responders' organisations from at least 3 different EU or Associated countries. Where applicable, Sub-topic: Open requires the active involvement of at least 6 such organisations, from at least 6 different EU or Associated countries.
SU-DRS04-2019-2020	Each RIA must establish its standard consortium agreement, as well as a "Collaboration Agreement" with participant(s) in the ENCIRCLE consortium. A draft of the "Collaboration Agreement" must be attached to the RIA proposal, and endorsed by at least one participant in ENCIRCLE. All beneficiaries of the RIA grant agreements must be independent from each beneficiary in the ENCIRCLE consortium. Each RIA proposal must be coordinated by an SME.
SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 6 such organisations, from at least 6 different EU or Associated countries.

SU-FCT03-2018-2019-2020	This topic requires the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries.
SU-FCT04-2020	Participation is required of at least 6 relevant practitioner organisations from at least 3 different EU or Associated countries.
SU-BES03-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES01-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 Border or Coast Guards Authorities from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 6 such organisations, from at least 6 different EU or Associated countries.
SU-BES03-2018-2019-2020	Consortia must be coordinated by a practitioner organization under civilian authority and command.
SU-GM01-2018-2019-2020	**For part a):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. Each proposal must include a plan, and a budget amounting at least 25% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions outside of the consortium, with a view to assessing the feasibility of their findings; 2. 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"); 3. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference 4. **part a)** is opened only in 2019. The Commission may, at the opening of the Call in 2019, provide more details about the professional areas eligible at the time, better to take account of the areas covered in previous Calls. **For part b), and c):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. 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"); 2. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference; 3. Only one network under each of part b), c) and d) may be supported over the 2018-2019 period. **For part d):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. Each consortium must commit to produce and update, every 12 or fewer months, a roadmap for both border and coast guards, and industry to plan ahead so as to facilitate investments into common, interoperable solutions for border security. 2. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference; 3. Only one such network may be supported over the 2018-2019 period.
SU-GM02-2018	Participation is required of at least 6 relevant practitioner organisations, as well as of 3 potential "buyers" of systems (e.g. departments or agencies dealing with acquisition planning, or procurement), from 3 different EU or Associated countries.
SU-GM03-2020, SU-GM04-2018-2019-2020	Participation is required of at least 3 relevant practitioner organisations, as well as of 3 potential "buyers" of systems (e.g. departments or agencies dealing with acquisition planning, or procurement), from 3 different EU or Associated countries.

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

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Consortium agreement:

	Members of consortium are required to conclude a consortium agreement, in principle prior to the signature of the grant agreement.

Call - Digital Security

H2020-SU-DS-2018-2019-2020

Cybersecurity and Digital Privacy

Cybersecurity and privacy technologies should become complementary enablers of the European digital economy, ensuring a secure and trusted networked environment for the governments, businesses, individuals and things, thus positioning EU as a world leader in building a more secure, privacy aware digital economy. The society as a whole will benefit from user-friendly cybersecurity and privacy systems, enabling an active participation of citizens and organisations to their own security and privacy. The compliance of the European infrastructures, products and services with relevant directives (e.g. NIS[12], eIDAS[13]), regulations (e.g. GDPR[14], proposal for an e-Privacy regulation) and standards (e.g. ISO27001, ISO27005) will promote trust and confidence to the European consumers and providers/suppliers, paving the way for a competitive, trustworthy Digital Single Market.

The Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[15] shaped the main related challenges and several strategic initiatives to address them. The Cybersecurity contractual Public Private Partnership (cPPP) was established in July 2016 aiming at building trust among Member States and industry by fostering cooperation at early stages in the research and innovation process and helping to align demand and supply. It has been an important mean of consultation providing input for H2020 Work Programme 2018-2020 and it will facilitate the engagement of end-users in sectors that are important beneficiaries and customers of cybersecurity solutions (e.g. energy, transport, health, finance) towards defining and providing to the industry their sector-specific digital security, privacy and data protection common requirements. The topics below belonging to this Digital Security call will be part of the contribution of the Commission to the cybersecurity cPPP.

SU-DS01-2018-2019: Cybersecurity preparedness - cyber range and economics

Specific Challenge: The digital infrastructure, upon which other sectors, businesses and society at large critically depend, must be resilient and trustworthy, and must remain secure despite the escalating cyber-threats. New technologies and their novel combinations require innovative ways to implement security measures, as well as making new security-related assumptions, identifying "zero day" vulnerabilities or potential unknown vulnerabilities, forecasting new threats plus their cascading effects and emerging attacks, as well as managing cyber risks.

Many organisations are unable to forecast and/or estimate the impacts (e.g. economic, reputational, legal, social, business, societal) of a cyber-risk (e.g. data breach). This results often

12 *TBC – reference to the NIS Directive*
13 *TBC – reference to the eIDAS Directive*
14 *TBC – reference to the GPD Regulation*
15 Brussels, 5.7.2016 COM(2016) 410 final.

in insufficient or wrong investments to ensure a more cybersecure environment. In addition, cybersecurity experts and professionals need to continuously adapt their expertise to a constantly evolving landscape comprising of increasingly sophisticated and novel cyber-attacks, a widening surface of exposed ICT systems and services and a set of relevant changing legislation. In a connected EU society, there is an urgent need for highly valuable cybersecurity professionals in such a complex and fast evolving field, and security experts need to be in a constant learning process, to match the quick rate of evolution of the cyber threats, attacks and vulnerabilities.

In addition, cybersecurity skills need to be continuously advanced at all levels (e.g. security officers, operators, developers, integrators, administrators, end users) in order to enable cybersecurity and digital privacy within the EU Digital Single Market.

Scope: Proposals are invited to address the sub-topics below, in 2018 and 2019.

Proposals should also address in each year specific social aspects of digital security related to education and training (particularly practical, hands-on training), including: (i) increase the dynamics of the education and awareness methods, to match/exceed the same rate of evolution of the cyber attackers; that is to say new methods of awareness/training offering more qualification tracks to fully and efficiently integrate ICT security workers and employers in the European e-Skills market; and (ii) integrate awareness into the eco-system of humans, competences, services and solutions which are able to rapidly adapt to the evolutions of cyber attackers or even surpass them.

Participation of SMEs is strongly encouraged.

Sub-topic 1 [2018]: Cyber range and simulation

As a continuation of topic DS-07-2017 "Addressing advanced cyber security threats and threat actors", where cyber range is partially addressed, proposals are called to focus on extended capabilities of cyber ranges (e.g. piloting of networked cyber-ranges; extension of the cyber-ranges network, adding domain specificities like cyber range for IoT and/or for Industrial Control Systems such as SCADA).

The proposals should develop highly customizable dynamic simulators serving as knowledge-based platforms accompanied with mechanisms for real time interactions and information sharing, feedback loops, developments and adjustments of exercises. These simulation platforms will help professionals responsible for cybersecurity in organizations to collaboratively improve their ability in handling and forecasting security incidents, complex attacks and propagated vulnerabilities, based upon targeted scenarios and exercises. Proposals are encouraged to bring shared approaches to express and transform user needs into actual experiments and cyber exercises (e.g. capture-the flag) and to develop/integrate/parameterise appropriate tools and methods (e.g. modelling, gaming, dynamic decision making, extended dynamic vulnerability databases, attack ontologies/taxonomies) for supporting current and future generated evidence-based simulation scenarios. The proposed cyber-range model should be validated across one critical economic sector, involving as many as possible relevant

stakeholders from its supply chain. Proposers are encouraged to create operational links to the CERTs / CSIRTs network across the EU.

Sub-topic 2 [2019]: Economics in cybersecurity and in data privacy

Proposals should develop operational ways to continuously analyse the information collected by CERT and/or CSIRT centres and all relevant cybersecurity data (e.g. open, proprietary, Big data). This analysis should feed their risk analysis models (which need to comply with relevant standards e.g. ISO27001, ISO27005 and relevant EU cybersecurity legislation) in order to derive appropriate econometric models that can be used by public/private organisations/companies (e.g. insurance companies, SMEs, governmental bodies). These econometric models should assist them to select realistic, affordable baseline cybersecurity measures that will improve their security, resilience and sustainability. These models should also help in identifying the cost and time to recover following a cyber-attack. In addition, the econometric models should be helpful for (a) identifying affordable security controls that are needed to protect valuable organization assets, (b) promoting the development of cyber insurance and liability policies/contracts and (c) fostering service level agreements addressing security and privacy requirements and policies. Proposals should bring innovative approaches to enforce and encourage accountability of security as a shared responsibility.

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

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

Expected Impact:

Sub-topic 1 - short-term : Professionals better prepared to detect, block and mitigate emerging cyberattacks; end users of cybersecurity products and services more involved into expressing actual needs to developers/vendors; more organized collaboration between a network of cyber-ranges and Europe-wide initiatives such as the CERTs/CSIRTs cooperation network of the NIS directive.

Sub-topic 1 - medium and long term: Improved resilience of ICT systems/infrastructures and reduced time and cost in infrastructures for training users; EU countries better prepared to face malware campaigns and to take down malicious infrastructures; improved EU-skills market.

Sub-topic 2 - short term: Improved risks analysis models to be used by public/private organisations; appropriate econometric models able to learn from cyber incident data on a wide scale; and improved knowledge on how organisations can make the right investment to secure their operations against cyber-attacks (e.g. personal data breaches).

Sub-topic 2 - medium and long term: Better preparedness to put in place cybersecurity measures and identify the necessary resources for recovering after a cyber-attack; Improved security, resilience and sustainability of organisations.

Type of Action: Innovation action

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

SU-DS02-2020: Management of cyber-attacks and other risks

Specific Challenge: To improve the security of an ICT system or of interconnected systems/infrastructures, additional security-related measures (e.g. components, processes, policies) should be incorporated, ensuring the main functions of security governance (investigation, detection, response, recovery, protection, forecast). Security management must use an integrated approach taking into account people, complex and interrelated processes and technologies, as well as the interrelationships among cybersecurity, privacy, accountability and resilience. While protective and preventive controls make life more difficult for attackers, organizations must constantly forecast, monitor and audit their systems (e.g. act on the assumption that attackers with different profiles have already penetrated their systems, and actively search for evidence - who, what, when, where and how). Within interconnected infrastructures, organizations/entities must collaborate and share evidence and information (including reporting to CERTs/CSIRTs) in order to better manage complex, cascading, interrelated threats and attacks as well as propagated vulnerabilities.

Another significant challenge is acquiring a larger share of the global cybersecurity products and services market, as this would be a clear indicator of success for EU security service providers.

Scope: Proposals should address at least one of the sub-topics below and there should be at least 2 proposals selected for each sub-topic.

Proposals should also address specific social aspects of digital security related to education and training (particularly practical, hands-on training), including: (i) increase the dynamics of the education and awareness methods, to match/exceed the same rate of evolution of the cyber attackers; that is to say new methods of awareness/training offering more qualification tracks to fully and efficiently integrate ICT security workers and employers in the European e-Skills market; and (ii) integrate awareness into the eco-system of humans, competences, services and solutions which are able to rapidly adapt to the evolutions of cyber attackers or even surpass them.

Participation of SMEs is strongly encouraged.

Sub-topic 1: Dynamic Governance, Risk and Compliance (GRC) promoting accountability and auditability.

Proposals should incorporate beyond state-of-the-art dynamic, evidence-based risk management, accountability, auditing and crowed sourcing technologies in pilots with significant scale and involving heterogeneous cyber systems interconnected infrastructures and cross-border digital services. Proposals should address inter-alia: risk-based situation awareness, real-time, evidence-based risk assessment, forecasting and real-time decision support. The proposals should (a) develop innovative dynamic, automated security management systems that identify the source/owner of the risk(s) (i.e. who is responsible for the vulnerability that was exploited e.g. internet provider, software developer, manufacturer, administrator) (b) develop/ integrate accountability technologies and mechanisms at all stages of the security management and (c) develop/integrate auditability mechanisms ensuring security and privacy of the proposed security governance solutions.

Sub-topic 2: Information sharing, security/privacy analytics and cyber-threat detection

Proposals should define, validate, demonstrate and exemplify advanced, integrated cyber-threat detection and intelligence concepts that could provide a pattern for products, managed security services and solutions throughout the EU and beyond.

Proposals should address at least two of the following strands:

Strand 1. Enhance cyber intelligence by developing collaborative, open, dynamic repositories of vulnerabilities in new technologies (e.g. IoT, Industrial Control Systems, Cloud technologies) in collaboration with CERTs/CSIRTs;

Strand 2. Advance existing cybersecurity ontologies and attack taxonomies helping the common understanding of security experts and forensics investigators in analysing open information linking to security incidents/evidence;

Strand 3. Develop/integrate/parameterise open-intelligence and Big data analysis and detections tools which will incorporate cybersecurity intelligence and leverage a variety of data sources and fields (e.g. cyber psychology) in order to optimise the detection/investigation of cybersecurity incidents;

Strand 4. Advance the accountability and auditing approaches/technologies in order to distribute security responsibilities.

Sub-topic 3: Advanced security solutions and services

Proposals should address technology, processes, and business-related aspects of building and running advanced cybersecurity services, including approaches to service quality assessment to support consumers or end users in their efforts to select digital services and providers. Proposals should also develop tools and device demonstrators addressing the security needs for heterogeneous applications and interconnected infrastructures and systems.

Proposals should address at least one of the following services: code auditing, provision of data boxes forensics, threat intelligence, certification and assurance, cyber insurance.

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

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

Expected Impact:

Sub-topic 1 - short term: The results will be helpful for the implementation of the NIS Directive in the Member States; efficient risk management, with reduced cost and improved efficiency for organizations and governments alike (thereby benefiting the general population).

Sub-topic 1 - medium and long term: Better standardization and automated assessment frameworks for secure networks; integrated holistic methodologies for combined information security, cybersecurity, safety, and reliability risk management will enable better informed decisions on security-related investments at the corporate and national level.

Sub-topic 2 - short term: Reduced number and impact of successful cyber-attacks as a result of high-quality, timely threat intelligence and early and accurate detection of attacks/breaches; more effective and timely co-operation resulting from the faster sharing of information and dissemination of threat information on a higher level of quality; availability of comprehensive security analytics and threat intelligence technology and services, fit for the purpose, affordable, and flexible to evolve and keep pace with escalating threats and with innovations in technology and practice.

Sub-topic 2 - medium and long term: A stronger and more competitive EU cybersecurity industry as a result of the standards/platform-based approach enabling creation of flexible best-of-breed solutions.

Sub-topic 3 - short term: The efforts will support the implementation of the NIS directive, in particular, enabling and shaping collaboration between service providers, CERT/CSIRTs, and other relevant organizations.

Sub-topic 3 - medium and long term: A more dynamic and innovative EU market in cybersecurity services and a stronger global market share for EU cybersecurity service providers, which will yield significant economic benefits for Europe and ensure reliable cybersecurity services for EU organizations.

Type of Action: Innovation action

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

SU-DS03-2019: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Specific Challenge: Some members of the digital society in the EU are more vulnerable as they are less prepared to confront cyber-attacks. The scale, the value and the sensitivity of personal data in the cyberspace are significantly increasing and citizens are typically uncertain about who monitors, accesses and modifies their personal data. Breach of privacy and data leakage may facilitate abuse by third parties, including cyber-threats such as coercion, extortion and corruption.

In order to protect the freedom, security and privacy of citizens in Europe, people should be enabled to assess the risk involved in their digital activities and configure their own security and privacy controls across these services. The citizens need to become capable in providing their permission/consent and/or give scalable privileges for accessing their personal data/devices/terminals and for being monitored (e.g. via cookies).

Most Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs) lack sufficient awareness and can only allocate limited resources -both technical and human- to counter cyber risks, hence they are an easier target (e.g. of ransomware attacks) compared with large organizations. Security professionals and experts working for SMEs&MEs need to be in a constant learning steep process since cybersecurity is a significantly complex and fast-evolving field. Taking into account the significant economic role of SMEs&MEs in the EU, tailored research to innovation should support cybersecurity for SMEs&MEs.

Scope: Proposals should address one of the following sub-topics:

Sub-topic 1: Protecting citizens' security and privacy

Proposals should bring innovative solutions to personal data protection, benefitting the security and privacy of the citizens, develop new applications and technologies in order to help citizens to better monitor and audit their security and privacy, enabling them to become more engaged and active in the fight against cyber and privacy risks.

These solutions should include innovative approaches, techniques and use-friendly tools for: (1) improving resilience against data breaches; (2) identifying and removing insulting/harmful content data; (3) exercising citizens' "right-to-be-forgotten"; (4) informing citizens about their privacy level at any moment of their digital activities; (5) protecting or providing privileges for any access/audit/interference with citizens' "smart terminals" or their Internet-based communications (e.g. instant messages, voice over IP); (6) developing on-line help-desks services or "one-stop-shop" informing, helping citizens in dealing with any security and/or privacy incident, and enabling them in reporting any cyber or privacy related incident. Such approaches need to build bridges/synergies with data protection authorities and CERTs/CSIRTs.

In addition, assurance and transparency about the digital security and privacy levels of the products and services should be easily accessed, identified and monitored by all citizens,

independently of their physical condition or ICT skills, by developing appropriate innovative solutions (e.g. cyber-labels, privacy seals, digital stamps, dynamic indicators).

This sub-topic could be linked with other relevant topics under LEIT-ICT, such us: "Security and privacy engineering for the assurance of resilience in evolving ICT systems" (ref. SU-ICT-01-[2018]); "Supporting the emergence of data markets and the data economy" (ref. ICT-20-[2018-20]).

Sub-topic 2: Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security and privacy

Proposers are encouraged to bring innovative approaches to increase the knowledge sharing in digital security across SMEs&MEs and between SMEs&MEs and larger providers. The user SMEs&MEs should be supported by democratizing access to tools and solutions of varied sophistication level, to allow SMEs&MEs to benefit from innovative targeted solutions addressing their specific needs and available resources, that are currently reserved to larger organisations (due to their cost and availability of internal expertise).

The proposals should develop targeted, user-friendly and cost-effective solutions enabling SMEs&MEs to: (a) dynamically monitor, forecast and assess their security and privacy risks; (b) become more aware of vulnerabilities, attacks and risks that influence their business; (c) manage and forecast their security and privacy risks in an easy/affordable way; (d) build on-line collaboration between SMEs&MEs associations and with CERTs/CSIRTs, enabling thus individual SMEs&MEs to report any incident.

In addition, tools and processes should be proposed to facilitate the participation of user SMEs&MEs in cyber-ranges for cybersecurity (e.g. for creating joint experiments reflecting their daily digital activities and services).

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

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

Expected Impact:

- Citizens and SMEs&MEs are protected and become active players in the Digital Single Market, including implementation of the NIS and data protection directives.
- Security and privacy become a shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.
- Reduced economic damage caused by harmful cyber-attacks and privacy incidents.

- Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.

Type of Action: Innovation action

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

SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks

Specific Challenge: The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity, hence a power outage can have direct impact on the availability of other services (e.g. transport, finance, communication, water supply) where backup power is not available or the power restoration time goes beyond the backup autonomy.

With the transition to a decentralised energy system, digital technologies are playing an increasingly important role in the EPES: they contribute reducing the energy consumption; they enable the integration of higher shares of renewables and promote a more energy efficient system. At the same time, with the growing use of digital devices and more advanced communications and interconnected systems, the EPES is increasingly exposed to external threats, such as worms, viruses and hackers, data privacy breaches and other vulnerabilities.

Without appropriate cyber-defence measures, systems access could be violated with the malware spreading over the system and may cause power outages, damages and cascading effects to interconnected systems, and energy services. Therefore, the EPES is currently facing a range of threats requiring an attentive evaluation of the cyber security risk that allows taking proper countermeasures. For example, the decentralisation process of the EPES will increase the number of access points (e.g. smart meters, IoT), hence increasing the exposure to cyberattacks. Also, the network protocols used by existing SCADA/ICS (Supervisory Control and Data Acquisition System/Industrial Control Systems) were designed in times when cybersecurity was not part of the technical specifications for the system design, hence if a hacker or worm can get access to any control system, it can exploit the protocol to disable or destroy most industrial controllers. On the other side, unlike IT systems, a control system in the EPES that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts. At the same time, with the decentralisation leading to a distributed energy system, the concept of microgrid/islanding is de facto acting and could be further exploited against cyber-attacks and cascading effects in the EPES.

In order to pursue the integration of the renewables and to benefit from the advantages brought by a modern digitalised electricity grid, there is a need for new security approaches detecting and preventing threats with severe impacts and to shield the electric system against cyber-attacks. Without an adequate strategy and measures to protect the energy system, and in

particular a decentralised EPES, from cyber-attacks, the energy transition would be more risky, more costly and possibly in danger.

Scope: The proposals shall demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders. The proposals shall demonstrate the resilience of the EPES through the design and implementation of adequate measures able to make assets and systems less vulnerable, reducing its expositions to cyberattacks. Different scenarios of attacks with the relative counteracting measures have to be designed, described and tested on the field to verify effectiveness. Depending on the specific application, the proposal shall apply measures to new assets or to existing equipment where data flows were not designed to be cyber protected (e.g. SCADA, ICS). The proposals shall implement the following series of activities concurring to make the electric system cyber secure: (i) defining cybersecurity design principles and standards with a set of common requirements to inherently secure EPES; (ii) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy provision supply chain); (iii) on that basis, designing a secure network architecture with defence in depth approach implementing segmentation and security levels mechanism considering a functional hierarchical model; (iv) implementing the measures in real life demonstration testing the cyber resilience of the system with simulation of different types of attacks and severity; and (v) demonstrating the effectiveness of the measures with a cost-benefit analysis.

The proposals shall also (i) develop security information and event management system collecting logs and other security-related documentation for analysis that can also be used for information sharing across operators of essential infrastructures and CERTs; (ii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and (iii) propose policy recommendations on EU exchange of information.

The dimension of a pilot/demonstrator within the proposal shall be at city level, involving generators, one primary substation, secondary substations and end users. The proposals shall include the following types of entities: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers.

The proposals may refer to Industry 4.0 and other proposals and/or projects dealing with cybersecurity in energy.

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

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

Expected Impact:

- Built resilience against different levels of cyber and privacy risks.

- Ensured continuity of the critical business energy operations.
- The energy sector is better enabled to easily implement the NIS directive.
- Increase the resilience of the electric system to different levels of attack.
- The cyber protection measures will be easily reconfigurable to new threats.
- A set of standards and rules for certification of cybersecurity components, systems and processes will be made available.
- Cyber protection policy design and uptake at all levels from management to operational personnel.
- Manufacturers are encouraged in providing accountability and transparency, enabling third parties monitoring and auditing the privacy and security of their energy devices and systems.

Drafting Comment: This topic is jointly funded by CNECT and ENER.

Type of Action: Innovation action

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

SU-DS05-2018-2019-2020: Digital security, privacy and accountability in critical domains/sectors

Specific Challenge: In critical vertical sectors, cybersecurity technologies deployed in several application domains should be aligned to the specific domain needs, linking the demand side and the supply side for such cyber technologies. In the context of an increased digitization and also of growing complexity of cyber-attacks, there are certain sectors identified as critical (e.g. in the NIS Directive) from the point of view of cybersecurity needs such as transportation, healthcare, finance. These sectors are important customers of cybersecurity solutions; hence it is of outmost importance to facilitate the engagement of end-users towards defining and providing sector-specific common requirements about digital security, privacy and data protection. Building security and privacy by design, principles and standards should be clearly defined to protect the critical infrastructures in these sectors.

For transportation domain (aviation, maritime, terrestrial sectors involving smart vehicles such as aircrafts, ships, trains, busses, cars…), security must be managed pro-actively over the system as a whole. This must also extend to include interfaces to critical supporting infrastructures such as communication networks and satellite systems. The complexity of the transport sector finds its roots in the diversity of components that build the solutions in use and the very long lifecycle of these components. The challenge is to migrate these solutions, systems, and infrastructures to a higher level of cybersecurity.

ICT enables the healthcare sector to provide efficient, effective, cross-border top-quality healthcare services improving the public healthcare. Healthcare operations, services and applications are provided via various interconnected Infrastructures (e.g. hospitals, healthcare centres), systems (e.g. body scanners, patients' records management systems, patients' monitoring systems), entities (e.g. insurance companies, pharmaceutical companies, banks, manufacturers, suppliers) and people (patients, healthcare providers, employers). Personalized medicine is on the brink of becoming a successful approach to treat diseases. This increases the complexity of the pharmaceutical supply chain and rises the importance of a zero error rate for the supply of personalized medications. Cybersecurity in this respect is safety critical and novel approaches are needed to assure traceability and zero error deliveries.

This interconnectivity reveals various threats, making the healthcare ecosystem vulnerable to catastrophic attacks with high impact to healthcare institutions and people's lives. The healthcare industry has seen a major rise in cyber-attacks over the past two years, and data breaches increasingly damage the healthcare industry as well as the privacy of the people. Vulnerable patients' records management systems can be attacked leaking private medical information (e.g. health records, prescriptions). Connected medical devices are increasingly used, in particular in wearables and home health monitoring devices transmitting data (e.g. embedded sensors measuring blood pressure, temperature heart rates glucose levels) over unsecure wireless networks from the patients' home to the hospitals exposing the privacy of the patients and resilience of the healthcare infrastructures.

Digital technologies are profoundly changing the financial sector. Cybersecurity and trust solutions are essential to make FINTECH (digital technologies for finance) possible and for the stability of the financial sector that has to respond to increasingly sophisticated cyber-attacks.

Scope: Proposals in this topic should develop cyber innovation-based pilots/demonstrators devoted to piloting solutions in the specific critical domains mentioned above. During the conception and development steps, critical domains specifics such as complexity of infrastructure and their large scale should be taken into account. These pilots/demonstrators will possibly use the transversal cyber infrastructures and capabilities developed in other R&I projects to demonstrate how the developed innovations can satisfy specific requirements in these key vertical sectors.

Proposals should also address specific social aspects of digital security related to education and training, including: (i) increase the dynamics of the education and awareness methods, to match/exceed the same rate of evolution of the cyber attackers; that is to say new methods of awareness/training offering more qualification tracks to fully and efficiently integrate ICT security workers and employers in the European e-Skills market; and (ii) integrate awareness into the eco-system of humans, competences, services and solutions which are able to rapidly adapt to the evolutions of cyber attackers or even surpass them.

Participation of SMEs is strongly encouraged.

Proposals are invited to address the following sub-topics.

At least 2 proposals will be selected for each of the sub-topics.

Sub-topic 1 (2018): Digital security and privacy in multimodal transport

Proposals addressing this sub-topic should tackle at least one of the following strands:

Strand 1: Secure access management for citizens to all types of vehicles. A European Single Transportation market requires a pan-European, seamless solution to access across mass, shared and individual mobility, which will bring added value to citizens. However the corresponding increased interconnection of smarter systems increases the vulnerability surface and therefore novel tailored approaches should be proposed (e.g. related to cybersecurity by design in transportation systems).

Strand 2: Assurance and protection against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities. Feasible solutions in practice should be addressed (e.g. holistic warning systems for complex interconnected transportation means), shielding the vulnerabilities that have severe impact and catastrophic propagation effects to the multimodal transport operations. Applicants should propose integrated, holistic approaches and tools for dynamically, automatically forecast and manage complex security and privacy incidents in the multimodal transport service and operation. Proposals should improve the security intelligence of treating complex multimodal transport security and privacy incidents, vulnerabilities and attacks (e.g. enhance vulnerability repositories, enhance the means for identifying upcoming vulnerabilities). Proposals should develop practical means for relevant on-line sharing information and distributing real-time security and privacy warnings to all stakeholders in the multimodal transport ecosystem (collaboration with CERTs/CSIRTs is highly encouraged).

Strand 3: Standardization to allow the quick adoption of cybersecurity best practices in the domain. Proposals might evaluate the feasibility of a security labelling for transportation.

Sub-topic 2 (2019): Digital security and privacy in healthcare ecosystem

Proposals responding to this sub-topic should contribute towards the practical implementation of relevant EU legislation (e.g. NIS, eIDAS and GDPR) in the healthcare complex ecosystem involving all stakeholders (e.g. security officers, ICT administrators, operators, auditors, developers, manufactures, integrators) of all entities in the healthcare ecosystem (e.g. healthcare organizations/centres, associations, ministries, insurance companies, patients, providers, manufacturers).

Proposals addressing this sub-topic should tackle at least two of the following strands:

Strand 1: In collaboration with all stakeholders in the healthcare ecosystem and CERTs/CSIRTs, develop dynamic vulnerability data basis for collecting, uploading, maintaining, and disseminating vulnerabilities of ICT-based medical systems, technologies, applications and services (enhancing the ICT generic ones e.g. NIST, MITRE). Build dynamic

taxonomies for medical-related attacks in order to become the basis for building healthcare cyber security incident management systems.

Strand 2: Dynamic, evidence based, sophisticated security and privacy risk assessment frameworks and tools that can deal with cascading effects of threats, and propagated vulnerabilities in interconnected healthcare infrastructures, entities, systems, supply chain services and applications (compliant with appropriate cybersecurity standards e.g. ISO27001, ISO27005, ISO28000).

Strand 3: Provide collaborative privacy-aware tools enabling healthcare stakeholders to access and share information (where its integrity is guaranteed), advise and provide best/good practices about incident handling through appropriate interaction with healthcare participants respecting their privacy.

Sub-topic 3 (2019): Digital security and privacy in finance

Proposals addressing this sub-topic should tackle at least one of the following strands:

Strand 1: Resilience enhancing technologies. Proposers are expected to further develop innovative approaches (such as e.g. encryption, cloud computing or distributed ledger technology,..) tailored the finance domain, ensuring that a proactive preparedness helps financial market participants and infrastructures to share information and better cope with technological shortfalls. Proposals should explore tools for making the exfiltration of data for attackers unattractive, both for ‘data at rest’ and 'data in transit'; and they should collaborate with CERTs/CSIRTs.

Strand 2: New/enhanced/parameterized automated collaborative ICT tools for insurance companies are needed in order to collect security, privacy and accountability requirements from their clients and upgrade their insurance and liability policies respecting the EU cybersecurity and privacy directives and legislation as well as cybersecurity standards (e.g. ISO27001, 27005).

Strand 3: Standardization to allow the quick adoption of cybersecurity best practices in the domain. Applicants should propose novel approaches for promoting common standards for conducting stress and resilience testing across systemic financial market infrastructures and institutions or for certifying companies/organizations that can perform accredited conformity tests.

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

The Commission considers that proposals requesting a contribution from the EU of between EUR 3 and 6 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact:

- The technological and operational enablers of co-operation in Response and Recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive. Enhanced protection against emerging novel advanced threats in transportation (short term).
- Advances in the state-of-the-art analysis of healthcare related cyber threats, attacks and vulnerabilities; Sound analysis of cascading effects of healthcare related cyber threats within the supply chain; Improved cybersecurity information sharing and collaboration among healthcare stakeholders and with CERTs/CSIRTs; More targeted and acceptable security management solutions addressing healthcare specificities (short term).
- Trigger the fast adoption of cybersecurity/privacy best practices in the financial industry (short term).
- Better response and recovery technologies and services that will help transportation organizations significantly reduce the impact of propagated and cascaded threats, vulnerabilities and breaches (medium term).
- Improved security governance of the healthcare and transport sectors (medium term).
- Greater and more mature EU cybersecurity market in the healthcare, transport and finance sectors (medium term).
- Reduce the impact of breaches with various levels of success in penetrating the defences (medium term).
- Better cybersecurity for multimodal transport standards that will trigger fast adoption of best practices in the transport industry (long term).
- Established trust chains among all entities in the healthcare and transport eco-systems; Better implementation of the relevant EU legislation (e.g. NIS, eIDAS, GDPR) in the healthcare ecosystem (long term).
- Activate insurance companies to become the "evangelists" for promoting cyber security and privacy protection in the whole EU economic ecosystem (long term).
- Enhanced protection against emerging novel advanced threats in the financial sector (long term).

Type of Action: Innovation action

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

SU-DS06-2019-2020: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Specific Challenge: In an increasingly digitized and interconnected world, cyber security and privacy represent major concerns for many countries/regions and there is a clear need to maintain international cooperation among global research and innovation communities dealing with cyber security and digital privacy. Therefore enhanced cyber cooperation and dialogue are needed both within the EU and beyond.

While some Coordination Actions have stemmed from previous H2020 Work Programs (e.g. with US and Japan), it would be useful to continue/extend these international activities, in order to promote global R&D&I in the areas of cybersecurity and digital privacy.

Scope: There are two strands foreseen:

Strand 1 (2019): International cooperation and coordination between the EU and the United States (US)

The proposals should aim at: (i) undertake activities on cybersecurity beyond the existing bilateral cooperation; (ii) identify relevant activities worldwide, in other countries and (global) regions; (iii) encourage and facilitate dialogue between the EU and US; (iv) promote research and innovation activities related to cyber-security and data privacy, driven by the EU principles.

Encourage and facilitate an exchange of views between the relevant EU and US stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges; identify and map the relevant legislation and policies in place stimulating the innovation and deployment of cybersecurity solutions.

Identify opportunities for future cooperation between the European research and innovation ecosystems (including standardisation) and policy makers and the corresponding institutional and private entities in US.

In line with the EU's strategy for international cooperation in research and innovation, international cooperation is encouraged, and in particular with international research partners involved in ongoing discussions and workshops with the European Commission. Legal entities established in countries not listed in General Annex A and international organisations will be eligible for funding only when the Commission deems participation of the entity essential for carrying out the action

Consideration should be given also to issues which might need a specific approach in cybersecurity (e.g. open source software).

Strand 2 (2020): Coordination of cybersecurity R&I strategies and actions within the EU and with Associated Countries.

Proposals should look for synergies between existing strategies, initiatives, programs, and actions in the area of cybersecurity and data privacy, in different sectors/domains, and should analyse their effectiveness towards improved cyber resilience.

Proposals should also identify emerging needs and opportunities in cybersecurity, elaborate scenarios for possible future policy interventions in the area, and propose actions to strengthen the cooperation at the EU, national and regional levels.

The Commission considers that proposals requesting a contribution from the EU of up to EUR 0.8 million for strand 1 and up to EUR 1.2 million for strand 2 would allow this area to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact:

- Better cooperation of cybersecurity R&D&I actions, and a coordinated development and integration of cyber-security strategies at the EU, national and regional levels
- Enhanced bilateral international cooperation of the EU and identified relevant activities.
- Identified synergies between existing strategies, initiatives, programmes and actions, as well as emerging needs and opportunities in the area of cybersecurity.
- Scenarios for possible future policy interventions and new actions for strengthened EU cooperation in the area of cybersecurity.
- Improved cooperation in cybersecurity and data privacy within and beyond the EU.
- Improved dialogue of the EU with other countries.
- Enhanced EU coordination on cybersecurity and data privacy.

Type of Action: Coordination and support action

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

Conditions for the Call - Digital Security

Opening date(s), deadline(s), indicative budget(s):[16]

Topics (Type of Action)	Budgets (EUR million)	Deadlines
Opening: 01 Mar 2018		
SU-DS01-2018-2019 (IA) SU-DS02-2020 (IA) SU-DS03-2019 (IA) SU-DS04-2018-2020 (IA) SU-DS05-2018-2019-2020 (IA) SU-DS06-2019-2020 (CSA)		
Overall indicative budget		

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and
- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

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

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

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme.

[16] The budget figures given in this table are rounded to two decimal places.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Consortium agreement:

	Members of consortium are required to conclude a consortium agreement prior to the signature of the grant agreement.

Other actions

1. Reviews of projects

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

Type of Action: Expert Contracts

Indicative budget: EUR 0.25 million from each yearly budget

2. Workshops, conferences, expert groups, communication activities and 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

Indicative budget: EUR 2 million from each yearly budget

SU-SST

Space Surveillance and Tracking.

[to be completed]

SU-STANDSEC

Support to a consortium comprising JRC as ERNCIP coordinator and CEN and CENELEC in cooperation with ETSI to address how to achieve timely standardization in the field of security, including through structural changes.

Legal entities:

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

European Committee for Standardization (CEN) - Brussels (Belgium)

European Committee for Electrotechnical Standardization (CENELEC) - Brussels (Belgium)

European Telecommunications Standards Institute (ETSI).- Valbonne (France)

Type of Action: Grant to identified beneficiary - Coordination and support actions

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

Indicative budget: EUR 1 million from the 2018 budget