EN

Horizon 2020

Work Programme 2018-2020

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

IMPORTANT NOTICE ON THIS WORK PROGRAMME

This Work Programme covers 2018, 2019 and 2020. The parts of the Work Programme that relate to 2020 (topics, dates, budget) have, with this revised version, been updated. The changes relating to this revised part are explained on the Funding & Tenders Portal.

(European Commission Decision C(2020)1862 of 25 March 2020)

Table of contents

Introduction

Horizon 2020 Interim Evaluation

This work programme part takes account of the results of the Interim Evaluation of Horizon 2020. The approach taken in the 2016-2017 work programme of requiring a minimum number of practitioners in a consortium is continued. This not only ensures that the research projects are attuned to the requirements of practitioners, but also reduces oversubscription. The involvement of SMEs is promoted including by introducing a topic requiring the coordinator to be an SME. Furthermore, the need to bring newly-developed technologies closer to the market is promoted through the application of Pre-Commercial Procurements. It should be noted that security research is challenge-driven; its main purpose is to develop new technologies and working methods that will help practitioners respond to emerging security threats. As a consequence, TRL levels in this work programme part are relatively high.

Open access to research data

Please note that grant beneficiaries under Horizon 2020 will engage in research data sharing by default, as stipulated in Article 29.3 of the Horizon 2020 Model Grant Agreement (including the creation of Data Management Plan). However, keeping in mind that all proposals under this work programme part will be subject to Security Scrutiny, the attention of the grant beneficiaries of this work programme part is drawn to the fact that they may find more appropriate to opt out of these arrangements. More information can be found under General Annex L of the work programme.

Societal aspects

Security as societal value is a guiding principle throughout this work programme part. All individual actions must be in compliance with the provisions of the Charter of Fundamental Rights of the European Union.[1]. When dealing with the development of technologies, it is recommended that actions consider the concepts of "privacy by design", "data protection by design", "privacy by default", and "data protection by default".

A 'Societal Impact Table' is a specific feature of this work programme part. The table puts an emphasis on societal aspects of security research. It checks whether the proposed security research meets the needs of and benefits society and does not have negative impacts on society. Applicants must fill in the 'Societal Impact Table' as part of the submission process. This table is taken into account during the evaluation under the 'Impact' criteria.

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

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF
[2] http://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf

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.

Sustainable Development Goals

The actions are expected to support Europe's endeavours to implement the Sustainable Development Goals (SDGs), particularly SDG 16 'Promote just, peaceful and inclusive societies'. Specific actions may also contribute to other SDGs such as SDG 11 'Make cities and human settlements inclusive, safe, resilient and sustainable'.

Possible synergies with defence research

Following up the EU Global Strategy in the security and defence area, the Commission adopted the European Defence Action Plan (EDAP)[3] followed by a Communication on the establishment of a European Defence Fund with two windows to support collaborative defence research (research window) and defence capability development programmes (capability window). The defence research window is already operational with funding opportunities under the Pilot Project and the launch of the Preparatory Action on Defence Research with the publication of a first call for proposals on 7 June 2017. As a first step in the implementation of the capability window the Commission put forward a proposal for a European defence industrial development programme under the current MFF from 2019-2020. Whereas activities under Horizon 2020 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[4]. Where necessary, actions should clearly demonstrate how they complement and do not overlap with actions undertaken under the Preparatory Action on Defence Research.

Possible synergies with other funding programmes

Project proposers should consider and actively seek synergies with, and where appropriate possibilities for further funding from, other relevant EU, national or regional research and innovation programmes (including Internal Security Funds, ERDF/ESF+, LIFE programme or the Instrument for Pre-accession Assistance [IPA II]), private funds or financial instruments (including EFSI).

Examples of synergies are actions that build the research and innovation capacities of actors; mutually supportive funding from different Union instruments to achieve greater impact and efficiency; national/regional authorities actions that capitalise on on-going or completed Horizon 2020 actions aimed at market up-take/commercialisation.

In order to explore options for synergies, project proposers could seek contact with national/regional managing authorities and the authorities who developed the Research and

3 COM(2016) 950.
4 http://eda.europa.eu/what-we-do/eda-priorities/research-technology

Innovation Smart Specialisation Strategies (RIS3).[5] For this purpose the 'Guide on Enabling synergies between ESIF, H2020 and other research and innovation related Union programmes'[6] may be useful. Horizon 2020 project proposals should outline the scope for synergies and/or additional funding, in particular where this makes the projects more ambitious or increases their impact and expected results. Please note, however, that while the increase in the impact may lead to a higher score in the evaluation of the proposal, the reference to such additional or follow-up funding will not influence it automatically.

Focus Area 'Boosting the effectiveness of the Security Union'

All actions under this work programme part contribute to the Focus Area 'Boosting the effectiveness of the Security Union' (see below).

Contribution to focus area(s)

Focus Area 'Boosting the effectiveness of the Security Union' (SU): EUR 721.39 million

5 http://s3platform.jrc.ec.europa.eu/map
6 http://ec.europa.eu/regional_policy/sources/docgener/guides/synergy/synergies_en.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 importance of the Security Union agenda has been highlighted in the Commission Communication of 20 April 2016[7] and by the subsequent appointment of a Commissioner for the Security Union. The majority of Member States depend entirely on Horizon 2020 to cover their needs for innovative security solutions, and it represents 50% of the overall public funding for security research in the EU.

At the core of research in this area is the development of new products to meet the needs of security practitioners. Research is not just about developing new technologies or applying emerging technologies, but also requires understanding phenomena such as violent radicalisation and the development of more effective policies and interventions. This means social sciences and the humanities will be involved.

To help end results correspond to real needs, research will generally require the involvement of security practitioners and those working with at-risk groups, for example fire and rescue services, police forces, border and coast guards, municipalities, social workers, educators and civil society actors. One challenge is segmentation of civil security industry largely into national markets. Progressive development of a single market also in this area can be expected to bring benefits of economies of scale, providing incentives to businesses to develop new solutions and lowering costs for purchasers. To facilitate supply and demand for new goods and services, innovative procurement (PCP, PPI) will be used.

The Focus Area will support implementation of the Security Union priorities: reacting to and recovering from natural and man-made disasters; preventing, investigating and prosecuting crime including organised crime and terrorism; improving border entry security; protecting infrastructure against natural and man-made threats, including cyber-attacks; digital security, privacy and data protection; and space-related research.

Focus area impacts:

- Reduced loss of life and reduced environmental, material and economic losses from natural and man-made disasters.
- Key infrastructure better protected against natural and man-made threats, including cyber-attacks.
- New products that meet the needs of security practitioners in the EU, including for investigating and prosecuting crime (including cybercrime) and terrorism.
- EU borders better secured against the entry of undesirable persons or goods.

[7] *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*, COM(2016) 230 final, 20.4.2016.

- Ensuring a secure and trusted networked environment for the governments, businesses and individuals, thus positioning the EU as a world leader in building a more secure digital economy.

- Support for EU and national policies related to security, including those focusing on prevention.

- Space-related research harnessed to support security.

- Better understanding of the complex and interrelated drivers and societal contexts of security challenges including in particular radicalisation and polarisation.

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, 3, 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 SME instrument, the SESAR Joint Undertaking and the ECSEL Joint Undertaking.

Call - Protecting the infrastructure of Europe and the people in the European smart cities[8]

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 to soft 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" are 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 personal data protection common requirements.

When a topic has eligibility and admissibility conditions which require the active involvement of specific entities (e.g.: operators), this means that these entities have to be participants and should be directly involved in the carrying out of the tasks foreseen in the grant. When a reference is made to "practitioners", the text refers to someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants should 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.

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[9]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

---

8 The Commission reserves the possibility under this call to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

9 http://eda.europa.eu/what-we-do/eda-priorities/research-technology

For grants awarded under these topics for Innovation Action and/or Research and Innovation Action, under the 2019-2020 calls, the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

All topics in this work programme part will be subject to security scrutiny.

The aim of this Call is to protect and improve the resilience of critical infrastructures and soft targets.

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, plants 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, assessment of physical and cyber risks, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs), and fast recovery after incidents, 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) assess in detail all aspects of interdependent physical (e.g. bombing, sabotage and attacks with a variety of weapons against installations, buildings and ships; plane or drone overflights and crashes; spreading of fires, floods, landslides, disastrous consequences of global warming, seismic activity, space weather, combined threats, etc.) and cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server, electronic interference, distributed attacks), and the cascading risks resulting from 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,

(c) develop improved real-time, evidence-based security management of physical and cyber threats, taking account of the ageing of existing infrastructure, and

(d) provide scenarios and recommendations for policy planning, engagement of the civil society, and investment measures encompassing all aspects of prevention-detection-response-mitigation

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 -, for the protection of first responders such as rescue teams, security teams and monitoring teams, and for ensuring service continuity.

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, oil rigs, offshore platforms), transport infrastructure (airports, ports, railways, urban multimodal nodes), communication infrastructures and ground segments of space systems, health services, e-commerce and the postal infrastructure, sensitive industrial sites and plants, and financial services.

In 2020, while keeping the coverage of the assessment of risks, prevention, detection, response and mitigation of consequences, proposals should also address the interrelations between different types of critical infrastructure with the objective of developing tools and methods to minimise cascading effects and allow rapid recovery of service performance levels after incidents.

When selecting for funding the proposals submitted in 2018 or 2019 or 2020, the Commission will take due account of similar projects financed in the previous years since 2016, with a view to cover the largest possible spectrum of installations. Each year, a list of infrastructures excluded from the Call will be published on the Funding and Tenders Portal.

Consortia should involve the largest variety of relevant beneficiaries, including infrastructure owners and 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[10] international cooperation is encouraged, and in particular with international research partners in the context of the International Forum to Advance First Responder Innovation[11] in which the Commission has decided to participate.

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.

Indicative budget: The Commission considers that proposals requesting a contribution from the EU of about EUR 7 to 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:

[10] COM(2012) 497.
[11] http://www.internationalresponderforum.org/

- 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.
- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.

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.
- 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 for the protection 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.
- Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- 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 and safe cities, including for public spaces[12]

Specific Challenge: In the cities, public spaces such as malls, open crowded gathering areas and events, and non-restricted areas of transport infrastructures, constitute "soft targets", that is potential, numerous targets spread across the urban area and subject to "low cost" attacks strongly impacting the citizens. The generation, processing and sharing of large quantities of data in smart cities make urban systems and services potentially more responsive, and able to act upon real-time data. On the one hand, smart cities provide for improving the security of open and crowded areas against threats (including terrorist threats) and risks, by leveraging wide networks of detection and prevention capabilities that can be combined with human response to crisis to enhance first responders' actions. On the other hand, the distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.

Scope: The security and good operation of a smart and safe city relies on interconnected, complex and interdependent networks and systems: public transportation networks, energy, communication, transactional infrastructure, civil security and law enforcement agencies, road traffic, public interest networks and services offered by public and private operators.

Such networks provide with an efficient infrastructure for detection resources and "big data" collection. The screening of such data are being used by security practitioners to enhance their capabilities and performances. For instance, crowd protection and the security of public and government buildings can be improved through the identification of threats or of crime perpetrators, and the early detection of dangerous devices or products; first responders may get quicker on site by calculating in real time the shorter possible route to the scene of disaster.

Proposals under this topic should develop and integrate experimentally, in situ, the components of an open platform for sharing and managing information between public and private service operators and security practitioners of a large, smart city. The proposed pilots should consider how to combine, inter alia:

- Methods to detect weapons, explosives, toxic substances
- Systems for video surveillance
- Methods to identify, and neutralize crime perpetrators whilst minimizing intrusion into crowded areas

In designing the platform, proposals should:

- involve actively the security actors of the city area, their coordination and governance;

[12] This topic complements other smart cities actions, including those under the European Innovation Partnership on Smart Cities and Communities.

- solve interoperability issues, and ensure the interconnection and integration of the city smart systems with the systems supporting the security practitioners locally, including through modelling and simulating their interdependence;

- enhance the security of city smart systems, notably in terms of access control (e.g. with digital security measures such as layered authentication and access), secure communication and data storage, and address their possible misuse by criminals;

- consider new concepts of operation resulting from novel monitoring methods, data provided by extensive networks of sensors and social media;

- consider mitigation strategies in the context of a variety of scenarios in order to increase resilience;

- integrate modules to simulate security incidents, and their consequences;

- integrate modules to measure the quantitative and qualitative impact of the platform on security;

- provide for the sharing, consolidation and analysis of multi-sourced data.

The proposals should also address at least one of the following key issues:

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

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

- Support and implementation of a common approach to securing and managing in a reliable and untamperable manner 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, in line with data protection legislation.

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.

Solutions are to be developed in compliance with fundamental rights, privacy and data protection, especially as the development of big data creates specific challenges. Therefore, full compliance with data protection legislations must be ensured in exploiting big data. 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.

Projects should also foresee activities and envisage resources for cooperating with other projects funded under this topic and with other relevant projects in the field funded by Horizon 2020.

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).
- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.
- 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).
- IoT ecosystems (rather than distributed IoT infrastructures) built 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).
- Novel concepts of operations taking account of mutiple, heterogeneous data sources and the social media.
- Novel tools and systemic approaches to protect citizens against threats to soft targets in a Smart City.
- Contribute to the implementation of the measures foreseen in the Action Plan to support the protection of public spaces (COM(2017) 612 final).

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 of Europe and the people in the European smart cities

Opening date(s), deadline(s), indicative budget(s):[13]

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				
SU-INFRA01-2018-2019-2020 (IA)	24.00			28 Aug 2018
Opening: 14 Mar 2019				
SU-INFRA01-2018-2019-2020 (IA)		22.00		22 Aug 2019
SU-INFRA02-2019 (IA)		16.00		
Opening: 12 Mar 2020				
SU-INFRA01-2018-2019-2020 (IA)			15.00	27 Aug 2020
Overall indicative budget	24.00	38.00	15.00	

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 2 operators of the chosen type of critical infrastructure operating in 2 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

[13] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

	out of the tasks foreseen in the grant. The participation of industry able to provide security solutions is required. The duration of the proposed activities must not exceed 24 months.
SU-INFRA02-2019	At least the local governments of 2 cities or metropolitan areas in 2 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. The duration of the proposed activities must not exceed 24 months.

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 Funding & Tenders Portal.

Grant Conditions:

SU-INFRA01-2018-2019-2020, SU-INFRA02-2019	For grants awarded under this call for Innovation Actions, the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

Consortium agreement:

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

Call - Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe[14]

H2020-SU-AI-2020

Artificial Intelligence (AI) refers to any machine or algorithm that is capable of observing its environment, learning, and that, based on the knowledge and experience gained, can take intelligent actions or propose decisions. [15] There are many different technologies that fall under this broad AI definition and they very much refer to machine learning, data science, robotics, internet of things and use of big data. Furthermore, many applications of AI have already started to appear in our everyday lives, from image recognition to machine translations or music generation, or very soon might become our reality, such as connected and autonomous vehicles or medical diagnostics. However, it is not always clear how best to foster innovation and how best to raise awareness about potential benefits and risks of this promising technology. This uncertainty can be a source of concern but is also a sign of opportunity.

To address the challenges and make the most of the opportunities offered by AI, the Commission published a European strategy[16] in April 2018.

The Commission proposed an approach that places people at the centre of the development of AI (human-centric AI) and encouraged the use of this powerful technology to help solve the world's biggest challenges, such as fighting crime and improving cybersecurity.

In order to improve the competitiveness of Europe in AI, it is necessary to map the existing research excellence and to boost and facilitate technology uptake. At the same time it remains indispensable to safeguard the strategic autonomy of the EU when developing security systems using AI technology by finding ways of embracing the opportunities offered by AI.

In December 2018, the Commission adopted a Communication on Working together for Artificial Intelligence [17] containing a Coordinated Action Plan, which has been drawn up jointly with Member States. With the Coordinated Action Plan, the Commission intends to maximise the impact of investment at the EU and national levels, encourage cooperation across the EU, exchange best practices, and support the EU's global competitiveness in this sector. Security aspects of AI are prominently present in all actions of the adopted plan, from research until putting such technologies on the market.

Furthermore, the Commission is committed to embed the discussion on the risks and opportunities associated to AI in a wider development strategy for security, taking into

---

14 The Commission reserves the possibility under this call to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

15 "Artificial Intelligence – A European Perspective", EUR 29425 EN, 2018.

16 COM(2018) 237.

17 COM(2018) 795 final.

account various scenarios, needs, gaps and alternatives that are specific to each area of security.

Moreover, under the next programming period beyond 2020, the Commission proposed to invest at least 1 billion EUR per year from Horizon Europe and the Digital Europe Programmes into AI based technologies.[18] With the Digital Europe Programme, the Commission has put forward for the first time a dedicated programme to reinforce the EU's digital capacities in key technologies that might be further complemented by other funding instruments such as the Internal Security Fund, the future Border Management Fund or by the European Structural and Investment Funds.

AI is also becoming a topic of interest for Law Enforcement Agencies (LEAs) in Europe. Many Member States and Associated Countries have on-going initiatives to modernize the work of LEAs in this sense. However, AI asks for a significant technical and financial investment, due to which smaller countries may lag behind. Bringing this issue at EU level provides several advantages, such as possible economy of scale, centralized solutions on the issue of huge amount of data needed, or development of EU standards in this domain.

In order to scale up AI capacities of LEAs across Europe, close their AI skills gap, create synergies and tackle more efficiently their major challenges, it is essential to reach a critical mass through a close cooperation among the LEAs, research teams and industry. In such a way, the initiative would pave the way for a possible future establishment of a European AI hub in support of Law Enforcement, as a gravitational point of all AI-efforts related to LEAs, which would also, among others, contribute per se to achievement, when appropriate, of a European Strategic Autonomy in this critical dimension.

Such a European AI hub for LEAs should build on the AI-on-demand platform and be, where appropriate, linked to it so as to facilitate sharing of new technologies and advances across domains.

In addition, such a hub would serve as a common reference testing and experiment facility (could be a virtual network of physical facilities) to test state-of-the-art technology in the context of LEAs, taking into account all the technical and non-technical constraints imposed by the field (economic, legal, structural, organizational,…). This hub could also include regulatory sandboxes, in order to test practical solutions in environments where the regulatory context might need to be adapted or defined.

A European AI hub would support LEAs by improving their daily work and quality of the tools they have, by increasing the protection of these tools and of LEA infrastructures, as well as by diminishing the number and impact of technologically sophisticated crimes. Thus, four interconnected aspects need to be addressed within this hub in order to exploit various possibilities of AI to provide full support to LEAs:

1- How can AI help LEAs in preventing, detecting and investigating criminal activities and terrorism and in monitoring borders?

[18] COM(2018) 795 final.

2- At the same time, in order to support LEAs in their work, how can the malicious use of AI tools for criminal activities and terrorism be prevented, including malicious use of the AI tools developed in point 1?

3- Then, how can the AI tools used by LEAs, including the ones in point 1, be protected against cyber threats and attacks?

4- Finally, how can AI help in protecting LEA infrastructures from cyber threats and attacks?

AI can bring benefits to cybersecurity and to the fight against crime, including cybercrime and terrorism, but will introduce new challenges as well, some of them related to the scarcity of high-quality datasets. To this end, a close cooperation of different national Law Enforcement and judiciary systems is necessary in order to secure the existence and availability of large enough and up-to-date high-quality datasets at a European level.

All topics in this call will be subject to security scrutiny.

Projects under this call are implemented through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied. Proposals shall therefore foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices. This task will contribute to the actual set-up of a European AI hub in support of Law Enforcement at a later stage.

Proposals are invited against the following topic(s):

SU-AI01-2020: Developing a research roadmap regarding Artificial Intelligence in support of Law Enforcement

Specific Challenge: As indicated in the Coordinated Plan on Artificial Intelligence and in the Cybersecurity Joint Communication [19], there is a need to better understand: how AI-based systems, services and products could enhance the objectives of the security sector; how AI technologies can be protected from attacks; how to address any potential abuse of AI for malicious purposes; how to establish cybersecurity requirements for AI. From the Law Enforcement point of view, these dimensions have to be analysed in a longer term, taking into account that the potential AI benefits for Law Enforcement Agencies (LEAs) are threefold, i.e., through: 1) proactive policing (from reactive to anticipative policing); 2) data analysis (e.g., connecting the dots, discovering criminal patterns and defragmenting LEA actions), and 3) identity checks (improving detection, targeting and interdiction).

Scope: Proposals under this topic should provide an EU AI roadmap for LEAs, meeting their specific operational and cooperation needs, by identifying, in a longer-term perspective: the key areas in which AI would be beneficial for LEAs, the key areas in which it could pose a threat to security, cybersecurity requirements for AI based technologies in use or to be used by LEAs as well as means of prevention and mitigation of malicious use of AI for criminal

[19] JOIN(2017) 450

activities. As such this project would not only need to continuously interact (in a cluster mode) with projects funded under SU-AI02-2020 and SU-AI03-2020 but also provide recommendations for further work to be done under Horizon Europe, Digital Europe, or the Internal Security Fund as well as for policy and market uptake. The objective is to develop a research roadmap that provides answers to, e.g., following questions: What are and will be the AI needs of LEAs in their daily work? What are the major research gaps in the area of AI in support of LEAs? What are the challenges that need to be addressed, both from the fighting crime, including cybercrime and terrorism, and from improving cybersecurity (re)actions? Which approaches might be desirable? What needs to be set up for test and evaluation? How to prevent and mitigate malicious use of AI for criminal activities and terrorism?

Starting from these considerations, proposals must demonstrate commitment to produce recommendations that are updated continuously, and at least every 6 months, about the following lines of actions: which AI based technologies, systems and solutions could support/enhance the work of LEAs and how, what the corresponding restraints (including ethical and legal) are, as well as related risks, security challenges and protection measures. The proposal shall provide specific real-life LEAs scenarios, examples and evidence supporting their recommendations. The proposing consortium is expected to incorporate relevant security practitioners, researchers, civil society organisations and LEAs.

As indicated in the Introduction of this call, proposals should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices.

The Commission considers that proposals requesting a contribution from the EU of around EUR 1.5 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: Short term:

- Effective contribution to the overall actions of this call;

Medium and longer term:

- In the longer term perspective, identification of key areas in which AI would be beneficial for LEAs, meeting their operational and collaborative needs, and of key areas in which it could pose a threat to security;
- A carefully planned roadmap in order for Law Enforcement to benefit as much as possible from the AI based technologies, systems, solutions, including their protection;
- Increased awareness regarding the state of the art and trends in AI-based criminal activities (short-, mid- and long-term).

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-AI02-2020: Secure and resilient Artificial Intelligence technologies, tools and solutions in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence

Specific Challenge: The increasing complexity of security challenges, as well as more and more frequent use of AI in multiple security domains, such as fight against crime, including cybercrime and terrorism, cybersecurity (re-)actions, protection of public spaces and critical infrastructure makes the security dimension of AI a matter of priority. Research is needed to assess how to mostly benefit from the AI based technologies in enhancing EU's resilience against newly emerging security threats (both "classical" and new AI supported) and in reinforcing the capacity of the Law Enforcement Agencies (LEAs) at national and at EU level to identify and successfully counter those threats. In addition, in security research, data quality, integrity, quantity, availability, origin, storage and other related challenges are critical, especially in the EU-wide context. To this end, a complex set of coordinated developments is required, by different actors, at the legislative, technology and Law Enforcement levels. For AI made in Europe, three key principles are: "interoperability", "security by design" and "ethics by design". Therefore, potential ethical and legal implications have to be adequately addressed so that developed AI systems are trustworthy, accountable, responsible and transparent, in accordance with existing ethical frameworks and guidelines that are compatible with the EU principles and regulations.[20]

Scope: Proposals under this topic should aim at exploring use of AI in the security dimension at and beyond the state-of-the-art, and exploiting its potential to support LEAs in their effective operational cooperation and in the investigation of traditional forms of crime where digital content plays a key role, as well as of cyber-dependent and cyber-enabled crimes. On the one hand, as indicated in "Artificial Intelligence – A European Perspective", AI systems are being and will increasingly be used by cyber criminals, so research into their capabilities and weaknesses will play a crucial part in defending against such malicious usage. On the other hand, Law Enforcement will increasingly engage in active usage of AI systems to reinforce investigative capabilities, to strengthen digital evidence-making in court and to cooperate effectively with relevant LEAs. Consequently, proposals should:

- develop AI tools and solutions in support of LEAs daily work. This should include combined hardware and software solutions such as robotics or Natural Language Processing, in support of LEAs to better prevent, detect and investigate criminal activities and terrorism and monitor borders, i.e., opportunities and benefits of AI tools and solutions in support of the work of Law Enforcement and to strengthen their operational cooperation.

[20] Special focus should be put on verifying the compatibility with:(1) Guidelines of the European Group on Ethics in Science and New Technologies (regulatory framework to be ready in March 2019), (2) General Data Protection Regulation (GDPR).

Building on existing best practices such as those obtained through the ASGARD project [21], proposals should establish a platform of easy-to-integrate and interoperable AI tools and an associated process with short research and testing cycles, which will serve in the short term perspective as a basis for identifying specific gaps that would require further reflection and development. This platform should, in the end, result in a sustainable AI community for LEAs, researchers and industry as well as a specific environment where relevant AI tools would be tailored to specific needs of the security sector, including the requirements of LEAs. Those AI tools would be developed in a timely manner using an iterative approach to define, develop and assess the most pertinent digital tools with a constant participation of end-users throughout the project. By the end of the project, the platform should also enable a direct access for Law Enforcement to an initial set of tools. Specific consideration should be given to the issue of setting an appropriate mechanism to enable a proper access to the relevant data necessary to develop and train AI based systems for security.

Proposals should also:

- develop cybersecurity tools and solutions for the protection of AI based technologies in use or to be used by LEAs, including those developed under this project against manipulation, cyber threats and attacks, and;

- exploit AI technologies for cybersecurity operation purposes of Law Enforcement infrastructures, including the prevention, detection and response of cybersecurity incidents through advanced threat intelligence and predictive analytics technologies and tools targeting Cybercrime units of LEAs, Computer Security Incident Response Teams (CSIRTs) of LEAs, Police and Customs Cooperation Centers (PCCCs), Joint Investigation Teams.

Finally, in order to have the full picture of all AI-related issues in the domain of work of Law Enforcement and citizen protection, proposals should:

- tackle the fundamental dual nature of AI tools, techniques and systems, i.e.: resilience against adversarial AI, and prevention and protection against malicious use of AI (including malicious use of the LEA AI tools developed under this project) for criminal activities or terrorism.

The improvement of research results, application and uptake should be taken into consideration.

The functionality of existing EU LEAs' tools and systems needs to be analysed since they need to support the prevention, reaction and detection of cyber threats and security incidents.

[21] ASGARD project - (http://www.asgard-project.eu/) aims to contribute to LEA Technological Autonomy, by building a sustainable, long-lasting community for LEAs and the R&D industry. This community will develop, maintain and evolve a best-of-class tool set for the extraction, fusion, exchange and analysis of Big Data, including cyber-offense data for forensic investigation. ASGARD helps LEAs significantly increase their analytical capabilities.

Furthermore, the accuracy of AI tools depends on the quantity and on the quality of the training and testing data, including the quality of their structure and labelling, and how well these data represent the problem to be tackled. In the security domain, this issue is further emphasized due to the sensitivity of the data, which complicates the access to real multilingual datasets and the creation of representative datasets. A huge amount of up-to-date high-quality data needed to develop reliable AI tools in support of Law Enforcement, in the areas of cybersecurity and of the fight against crime, including cybercrime and terrorism, asks for the development of training/testing datasets at a European level. This requires a close cooperation of different national Law Enforcement and judiciary systems. Namely, training and testing data sets considered legal and used in one country have to be shared and accepted in another one, while simultaneously observing fundamental rights and substantial or procedural safeguards. The lack of legislation at the national and international level makes this particularly difficult. The availability of such datasets to the scientific community would ensure future advances in the field.

Thus, in order to address the problem of securing European up-to-date high-quality training and testing data sets in the domain of AI in support of Law Enforcement, proposals under this topic should, from a multidisciplinary point of view, identify, assess and articulate the whole set of actions that should be carried out in a coherent framework:

- A comparative analysis of existing legal provisions throughout Europe that apply in these cases and their impact, including obstacles for research community to access datasets used by LEAs and means of overcoming these obstacles;
- The identification and definition of legislative changes that could be promoted both at the European and Member State level;
- Ethical and operational implications for LEAs;
- The identification of the technical developments that should be carried out to sustain all these aspects;
- Determination of legal and ethical means at the European level that allow for a creation of European up-to-date, representative and large enough high-quality training and testing data sets for AI, in support of Law Enforcement and available to the scientific community working with LEAs.

Proposals should have a clear dissemination plan, ensuring the uptake of project results by LEAs in their daily work.

Taking into account the European dimension of the topic, the role of EU agencies supporting Law Enforcement should be exploited regarding:

- effective channels established between industry and LEAs, closing the gap between public investment and uptake of project results by relevant end-users in their daily work;

- increased exchange of experiences, best practices and lessons learnt throughout Europe leading to EU common approaches for opportunity/risk assessment of AI;
- better understanding and readiness of policy makers on future trends in AI;
- enhanced cooperative operations and synergies between EU LEAs.

Proposals should take into account the existing EU and national projects in this field, as well as build on existing research and articulate a legal, ethical and practical framework to take the best out of the AI based technologies, systems and solutions in the security dimension. Whenever appropriate, the work should complement, build on available resources and contribute to common efforts such as (but not limited to) ASGARD, SIRIUS[22], EPE[23], networks of practitioners [24], AI4EU[25], or activities carried out in the LEIT programme, namely in Robotics[26], Big Data[27], and IoT[28]. As proposals will leverage existing technologies (open source or not), they should show sufficient triage of these technologies to ensure no internalisation of Intellectual Property Rights or security risks as well as demonstrate that such technologies come with adequate license and freedom to operate.

As far as the societal dimension is concerned, proposed solutions of AI applications should respond to the needs of an individual and society as a whole by building and retaining trust. Proposals should analyse the societal implications of AI and its impacts on democracy. Therefore, the values guiding AI and responsible design practices that encode these values into AI systems should also be critically assessed. It should be also shown that the testing of the tools represents well the reality. In addition, AI tools should be unbiased (gender, racial, etc.) and designed in such a way that the transparency and explainability of the corresponding decision processes are ensured, which would, amongst other, reinforce the admissibility of any resulting evidence in court.

Proposals' consortia should comprehend, besides industrial and research participants, relevant security practitioners, civil society organisations, experts on criminal procedure from a variety of European Member States and Associated Countries as well as LEAs. Proposals should ensure a multidisciplinary approach and have the appropriate balance of IT specialists as well as Social Sciences and Humanities experts.

As indicated in the Introduction of this call, proposals should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices.

---

22 SIRIUS, launched by Europol in October 2017, is a secure web platform for law enforcement professionals in internet-facilitated crime investigations, with a special focus on counter-terrorism.

23 EPE (Europol Platform for Experts) is a secure, collaborative web platform for specialists in a variety of law enforcement areas.

24 Such as ILEAnet (https://www.ileanet.eu/) and I-LEAD (i-lead.eu/)

25 developing the AI-on-demand platform, central access point to AI resources and tools: http://ai4eu.org/.

26 For instance exploiting technology developed in H2020 robotics projects in Search and Rescue, support to civil protection, or inspection and maintenance - https://eu-robotics.net/sparc/

27 http://www.bdva.eu/ppp-projects - such as AEGIS, Lynx or FANDANGO.

28 MONICA, SecureIoT.

The Commission considers that proposals requesting a contribution from the EU of around EUR 17 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: Proposals should lead to:

Short term:

- Effective contribution to the overall actions of this call;
- Development of a European representative and large enough high-quality multilingual and multimodal training and testing dataset available to the scientific community that is developing AI tools in support of Law Enforcement;
- EU common approach to AI in support of LEAs, centralized efforts as well as solutions on, e.g., the issue of huge amount of data needed for AI.

Medium term:

- Improved capabilities for LEAs to conduct investigations and analysis using AI, such as a specific environment/platform where relevant AI tools would be tailored to specific needs of the security sector including the requirements of LEAs;
- Ameliorated protection and robustness of AI based technologies against cyber threats and attacks;
- Raised awareness and understanding of all relevant issues at the European as well as national level, related to the cooperation of the scientific community and Law Enforcement in the domain of cybersecurity and the fight against crime, including cybercrime and terrorism regarding the availability of the representative data needed to develop accurate AI tools;
- Raised awareness of the EU political stakeholders in order to help them to shape a proper legal environment for such activities at EU level and to demonstrate the added value of common practices and standards;
- Increased resilience to adversarial AI.

Longer term:

- Improved capabilities for trans-border LEA data exchange and collaboration;
- Modernisation of work of LEAs in Europe and improvement of their cooperation with other modern LEAs worldwide;
- A European, common tactical and human-centric approach to AI tools, techniques and systems for fighting crime and improving cybersecurity in support of Law Enforcement, in full compliance with applicable legislation and ethical considerations;

- Fostering of the possible future establishment of a European AI hub in support of Law Enforcement, taking into account the activities of the AI-on-demand platform;
- Making a significant contribution to the establishment of a strong supply industry in this sector in Europe and thus enhancing the EU's strategic autonomy in the field of AI applications for Law Enforcement;
- Creation of a unified European legal and ethical environment for the sustainability of the up-to-date, representative and high-quality training and testing datasets needed for AI in support of Law Enforcement; as well as for the availability of these datasets to the scientific community working on these tools;
- Development of EU standards in this domain.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 7-8; please see part G of the General Annexes.

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-AI03-2020: Human factors, and ethical, societal, legal and organisational aspects of using Artificial Intelligence in support of Law Enforcement

Specific Challenge: Advantages of AI are numerous. However, the lack of transparency of AI technologies and tools complicates their acceptance by users and citizens. Ethical and secure-by-design algorithms are necessary to build trust in this technology, but a broader engagement of civil society on the values to be embedded in AI and the directions for future development is crucial. This fact is generally correct, and it becomes extremely important in the security domain. Social engagement has to be part of the overall effort to fortify our resilience across institutions, civil society and industry, and at all levels - local, national, European. There is a need to find ways to build a human-centred and socially driven AI, by, amongst other, fostering the engagement of citizens and improving their perception of security. Possible side effects of AI technological solutions in the domain of security need to be considered carefully, both from the point of view of citizens and from the point of view of Law Enforcement: e.g., their concerns regarding a strong dependence on machines, risks involved, how AI will affect their jobs and their organisation, or how AI will affect their decisions. Many open aspects exist that can be a source both of concern and of opportunity and should be addressed in a comprehensive and thorough manner. Finally, the legal dimension should be tackled as well – e.g., how the use of data to train algorithms is dealt with, what is allowed and under which circumstances, what is forbidden and when.

Scope: Proposals under this topic should provide an exhaustive analysis of human, social and organisational aspects related to the use of AI tools, including gender related aspects, in support of Law Enforcement, both for cybersecurity and in the fight against crime, including cybercrime, and terrorism. Points of view and concerns of citizens as well as of Law

Enforcement should be tackled. Based on this analysis, proposals should suggest approaches that are needed to overcome these concerns and that stimulate the acceptance of AI tools by civil society and by Law Enforcement. Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of privacy, protection of personal data and free movement of persons. The societal dimension should be at the core of the proposed activities. Proposals should be submitted by consortia involving relevant security practitioners, civil society organisations as well as Social Sciences and Humanities experts.

As indicated in the Introduction of this call, proposals should foresee resources for clustering activities with other projects funded under this call to identify synergies and best practices.

The Commission considers that proposals requesting a contribution from the EU of around EUR 1.5 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: Proposals should lead to:

Short term:

- Effective contribution to the overall actions of this call.

Medium term:

- Improved and consolidated knowledge among EU Law Enforcement Agency (LEA) officers on the issues addressed in this topic;
- Exchange of experiences among EU LEAs about human, social and organisational aspects of the use of AI in their work;
- Raised awareness of civil society about benefits of AI technologies in the security domain and opportunities it brings.

Longer term:

- European common approach for assessing risks/threats involved by using AI in the security domain, and identifying and deploying relevant security measures that take into account legal and ethical rules of operation, fundamental rights such as the rights to privacy, to protection of personal data and free movement of persons;
- Advances towards the implementation of the AI tools and technologies in support of Law Enforcement, in the areas of cybersecurity and fight against crime, including cybercrime, and terrorism, by strengthening the civil society perception of the EU as an area of freedom, justice and security.

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 - Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe

Opening date(s), deadline(s), indicative budget(s):[29]

Topics (Type of Action)	Budgets (EUR million)	Deadlines
	2020	
Opening: 12 Mar 2020		
SU-AI01-2020 (CSA)	1.50	27 Aug 2020
SU-AI02-2020 (IA)	17.00	
SU-AI03-2020 (CSA)	1.50	
Overall indicative budget	20.00	

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-AI01-2020	This topic requires the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries. The duration of the proposed activity must not exceed 60 months.

[29] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

SU-AI02-2020	This topic requires the active involvement of at least 5 Law Enforcement Agencies (LEAs) from at least 5 different EU or Associated countries. The duration of the proposed activity must not exceed 60 months.
SU-AI03-2020	This topic requires the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries. The duration of the proposed activity must not exceed 24 months.

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 Funding & Tenders Portal.

Grant Conditions:

SU-AI02-2020	For grants awarded under this topic the beneficiaries must grant access rights for EU institutions, bodies, offices or agencies and Member States under the special conditions for the Specific Objective 'Secure societies - Protecting freedom and security of Europe and its citizens'. The respective option of Article 31.5 of the Model Grant Agreement will be applied.
SU-AI01-2020, SU-AI02-2020, SU-AI03-2020	For grants awarded under these topics the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.
SU-AI01-2020, SU-AI02-2020, SU-AI03-2020	Grants awarded under the Artificial Intelligence call will be implemented through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied.

Consortium agreement:

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

Call - Security[30]

H2020-SU-SEC-2018-2019-2020

This Call deals with R&D and innovation towards establishing disaster-resilient societies, fighting against crime and terrorism, and improving border and external security.

When a topic has eligibility and admissibility conditions which require the active involvement of specific entities (e.g.: '3 Law Enforcement Agencies (LEA) from at least 3 different EU or Associated countries'), this means that these entities have to be participants and should be directly involved in the carrying out of the tasks foreseen in the grant. When a reference is made to "practitioners", the text refers to someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants should 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.

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[31]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

For grants awarded under these topics for Innovation Action and/or Research and Innovation Action, under the 2019-2020 calls, the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

All topics in this work programme part will be subject to security scrutiny.

Disaster-Resilient Societies

Securing itself against, and being prepared for, disasters is one of the central elements of the functioning of any society. There are hardly any societal functions which are not to some extent exposed to natural or man-made disasters and related resilience and security issues.

---

30 The Commission reserves the possibility under this call to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

31 http://eda.europa.eu/what-we-do/eda-priorities/research-technology

The aim of this section is to advance innovation in the society at large, and among first responders (as acknowledged within the International Forum to Advance First Responder Innovation[32] *in which the Commission has decided to participate) to reduce the loss of human life and to reduce environmental, economic and material damage from natural and man-made disasters, including from climate-related weather events, earthquakes and volcanic events, space 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, and how governments and civil society organisations design and implement policies for mitigating risks, preparing for, reacting to, overcoming, and learning from disasters. The spread of new technologies and media are inducing dramatic changes in how individuals and communities behave, and they are affecting societies in unpredictable ways. Building the resilience of society and citizens requires a better understanding and implementation of these new technologies, media and tools, and their capacity to raise disaster risk awareness, to improve citizen understanding of risks, to build a culture of risks in society, to enable an effective response from affected populations, to improve functional organisation in most fragile and vulnerable environments, and to increase the resilience of health services, social services, education, and governance, in line with target (d) of the Sendai Framework on critical infrastructure and disruption of basic services.

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

Recent disasters related either to natural causes (including climate-related hazards) or to terrorist attacks have shown gaps in the level of preparedness of European society for disasters, and therefore highlighted the importance of increasing risk awareness, and hence resilience among people and decision-makers in Europe. There is much that can be learned from certain countries with a high level of risk of natural disasters (e.g. Japan with high-levels of risks of earthquakes, volcanic events, and tsunamis) and where risk awareness is high. Research is required with a view to how cultural changes among individuals, business managers, government officials, and communities can create a resilient society in Europe, in line with the Sendai Framework for Disaster Risk Reduction.

Over the past few years several ways to exploit social media and other crowd-sourced data in emergency situations have been studied, and some put in place, but their impacts 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 should analyse both the positive and negative roles of social media and crowd-sourced data in crisis situations. For instance in the wake of a terror attack or natural disaster they offer a quick and easy way to relieve friends

[32] *http://www.internationalresponderforum.org/*

and family from worry (where networks are not down), and they generate valuable information about the affected area in the first moments after a disaster; they have been used to spread early warnings and important safety information. However, social media may also be used to spread false statements and to overstate threats, so the validation processes of information should also be addressed. Social media itself is reliant upon the functioning of critical infrastructure such as phone networks and may not always be available. Research should also address solutions for communication between first responders and the victims and citizens in the affected area.

Research on risk awareness should encompass the whole of the disaster management cycle, from prevention (e.g. through education) and preparedness (knowing how to react), emergency management (collaboration and communication before and during an event), response (empowering citizens to act efficiently by themselves according to more effective practices and following established guidelines), and recovery (knowledge to build back better). Researchers should take into account tangible and intangible cultural heritage, traditional know-how, land use, construction technologies, and other local knowledge which is a valuable source of information for the local communities and can help prevent the creation of new risks, to reduce existing risks, to prepare for and to respond to disasters and to build back better.

Sub-issues to be addressed are diversity in risk perception (as a result of e.g. geography (within Europe), attitudes, institutional and social trust, gender and socio-economic contexts), in vulnerabilities and in understanding responses to crises in order to propose new approaches and strategies for community awareness, for leadership, and for crisis readiness and management with a particular emphasis on the use of new technologies.

For achieving disaster-resilient societies that cope with disasters and build back better, the research community needs to transfer research outputs in an appropriate manner to meet citizen expectations given the current levels of risk acceptance, risk awareness, and involvement of civil society organisations in a mediating role.

Civil society organisations, first responders, (national, regional, local, and city) authorities are invited to propose strategies, processes, and methods to enable citizens better to access research results related to disaster resilience, and to prepare the ground for exercises involving citizens. These strategies, processes, and methods should be tested with citizens and communities 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 and communities.

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 crowd-sourced data, and the involvement of 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).

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 through multidisciplinary projects confronting different schools of thoughts. 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 the European diversity in terms of risk-perception amongst citizens, and of vulnerabilities;
- Comparative analysis of different approaches to adapt to, and be prepared for risks in different countries (both within and outside the European Union), and among communities in precarious socio-economic conditions;
- Advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals;
- Identification of existing tools and guidelines for an improved prevention (including risk understanding and communication), preparedness (including training involving citizens), alert systems and their recognition by citizens, responses using citizen's competencies and local knowledge, and recovery;
- 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 and non-urban environments, including in areas where precarious socio-economic conditions prevail;
- Intensive sharing, among communities, of good practices and of learnings resulting from citizen-scientist interaction;
- A consolidated, common European understanding of disaster resilience.

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 authorities to take proper measures in response to severe disasters, both natural (including climate-related extreme events) and man-made. 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 (cross-sectoral) needs of first responders.

Scope: Proposals are invited to propose novel solutions improving the protection of first responders against multiple and unexpected dangers, or enhancing their capacities by addressing 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 all sorts of disasters of natural, accidental, or man-made or of terrorist origins is a major issue for first responders. Novel technologies should 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 and reducing injuries.

- 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, as well as tools for joint epidemiological and criminal risk and threat assessment and investigation.

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

Development of innovative tools, methodologies and European pre-hospital guidelines for first responders of medical services, fire services and police and hospital trauma teams in order to ensure faster and more effective evaluation and control of numerous seriously injured casualties in disaster and/or emergency situations. This should take account of lessons learned from military mass-casualty techniques such as damage-control surgery. The aim is to ensure more effective pre-hospital triage of victims with appropriate digital traceability of actions and data transfer from the event to the hospital(s), including across administrative and political boundaries.

If appropriate, proposals should demonstrate how they will build on relevant previous and on-going FP7 and/or H2020 projects.

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

Other technologies for use by first responders may be subject of proposals provided that they involve a large number of first responders' organisations (see eligibility and admissibility conditions.) For instance, but not exclusively: communicating and smart wearables for first responders and K9 units including light-weight energy sources; situational awareness and risk mitigation systems for first responders using UAV and robots, connected and swarms of

drones; systems based on the Internet of Things; solutions based on augmented or virtual reality; systems communication solutions between first responders and victims; risk anticipation and early warning technologies; mitigation, physical response or counteracting technologies; etc.

Any novel technology or methodology under this topic should be tested and validated, not just in laboratories but also in training installations and through in-situ experimental deployment. They therefore need to be quick to deploy, bases on resilient and robust communication infrastructure. First responders, including through interdisciplinary teams (e.g. involving medical emergency services, public health authorities, law enforcement team, civil protection professionals, etc.) need to 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, fundamental rights and applicable legislation, including in the area of privacy, personal data protection and free movement of persons. Societal aspects (e.g. perception of security, possible effects of technological solutions on societal resilience, gender diversity) 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 Japanese or Korean research centres. Co-funding opportunities from the Japan Science and Technology Agency exist for Japanese partners.[33] Co-funding opportunities from the Korean MSIP/NRF exist for Korean partners.[34]

The centre of gravity for technology development with actions funded under sub-topics 1,2 and open is expected to be up to TRL 4 to 6, whereas under sub-topic 3 it 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 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, guidelines and methods aimed at facilitating their operations

[33] For more information on Japan, please consult http://www.jst.go.jp/sicp/announce_eujoint_04_GeneralInfo.html.

[34] For more information on Korea, 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=.

- 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 that is highly fragmented (because of the lack of standardization and harmonised certification), and 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 whole field of "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-standardisation, in particular:

- Sub-topic 1: [2018] 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 should be designed. Testing facilities should 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, including methods to monitor reservoirs, and sea or river levels for early warning.

- Sub-topic 2: [2019] Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)

Generally speaking, the development of standards for civil protection in the areas of crisis management (including for systems, tools and services related to natural hazard and CBRN-E emergencies) will increase interoperability of equipment and procedures. Innovation actions should bring validated and positively-assessed practices into standards within or outside current standardisation processes. The involvement of well-established standardisation

organisations is required. The complementarity of the proposed activities with activities supported by the European Defence Agency (EDA) in the CBRN-E area should be described comprehensively.

- Sub-topic 3: [2020] First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means

Improved standards and common communication data exchange mechanisms are required for an effective deployment of resources during the run-up to a major crisis related to any kind of disaster either natural (including resulting from climate-related extremes) or man-made, and immediately after the event, for example in case of a mass evacuation from an urban area. Proposals should target in particular events where there are strong cross-sector, cross-border, cross-hierarchy coordination activities ongoing, and therefore the issue of interoperability. The aim is to pave the way to improved standards, including voluntary Standard Operating Procedures (SOPs) and/or ISO or EN 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:

- [2018] full awareness of water supply facilities about the necessity of designing monitoring networks capable of detecting both contamination risks (safety) and deliberate poisoning (security);
- [2019] standards for interoperable equipment and procedures in the area of crisis management and civil protection (including natural hazard and CBRN-E emergencies in support to operations involving international crews;
- [2020] standards for an effective deployment of resources to respond to major crisis.

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 2017. 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.

Where applicable, the complementarity of the proposed activities with activities supported by the European Defence Agency (EDA) should be described comprehensively.

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.

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*[35] *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).

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

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-DRS05-2019: Demonstration of novel concepts for the management of pandemic crises

Specific Challenge: Large-scale pandemics constitute an ever growing threat in today's globalized society, given the increasing flows of goods and people among continents. This challenge ought to be addressed internationally, and with the involvement of a large variety of practitioners and stakeholders, from planners in national health systems, to first responders. The Horizon 2020 work programme separately includes an EIC Horizon Prize for 'Early Warning for Epidemics' that is relevant for preparedness and response specifically to vector-borne disease outbreaks.

Scope: In 2014 an exploratory phase was called for (in DRS4 of the 2014 Call in Societal Challenge 7) to address the feasibility of strengthening capacity-building for health and security protection in case of large-scale pandemics (phase 1). The resulting project has issued a range of recommendations for research gaps to be addressed in priority. It has also proposed innovative concepts to integrate better the existing tools and systems for health and security protection in case of large-scale pandemics, taking into account potential impacts of climate change.

All these recommendations and proposals will be made public on the portal of the Call in due time.

Demonstrations are now required to assess these novel concepts, in support of cross-border emergency approaches (phase 2), to strengthen preparedness and response to pandemics (including the detection of disease outbreaks that could lead to pandemics), in line with Decision 1082/2013/EU on serious cross-border threats to health[36] and the International Health Regulations (WHO, 2005)[37].

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.

Expected Impact: Short term:

- Novel concepts for health and security protection in the case of large-scale pandemics, validated by international organisations and a large number of EU Member States including a commitment to sharing these novel concepts.

[36] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013D1082
[37] http://www.who.int/topics/international_health_regulations/en/

- A prototype IT system integrating innovative tools, and supporting existing emergency frameworks.

- An operational strategy for implementation of the concepts and IT system supporting cross-border preparedness and crisis management, and demonstrated in situ.

Type of Action: 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

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 and CBRN-E attacks), along with understanding and tackling terrorist ideas and beliefs. Human factors and the societal context should be taken into account, whilst respecting fundamental rights, including privacy, protection of personal data and the free movement of persons.

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, globalised communication and finance infrastructure, provides many opportunities to its people. However, the benefits come along with risks related to crime and terrorism, a significant number of which have 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 play its part to help prevent, investigate and/or mitigate the impact of criminal acts, whilst protecting fundamental rights. 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 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 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 to exclude approaches that have previously failed. The societal dimension of fight against crime and terrorism should 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, 2020] New methods to prevent, investigate and mitigate trafficking of human beings and child sexual exploitation – and on the protection of victims**

Globalisation and technological developments facilitate trafficking in human beings and child sexual exploitation. A variety of preventive measures, as well as measures to ensure adequate victim protection and assistance are needed, that build upon advances in social sciences and humanities.

Proposals in this subtopic should address both phenomena in a balanced way. They should ensure that the research focuses on prevention, investigation and/or assistance related to all victims of trafficking and not only addressing child trafficking. In the same way, the proposals should cover any area concerning prevention, investigation and/or assistance to victims of child sexual exploitation, not only the assistance to victims of child sexual exploitation resulting from trafficking.

With respect to the trafficking of human beings, research should bear on:

- preventing the phenomenon and to reduce the demand for all forms of exploitation in the trafficking chain and its legal and illegal sectors. The analysis of possible involvement of organized crime groups implicated in trafficking of human beings in other crimes as well (e.g., financial crimes) is recommended;
- new approaches to investigate cases involving the trafficking of human beings;
- new approaches to mitigate the impact on victims in the short and long term.

Regarding child sexual exploitation:

- how to address new threats, such as live-streaming of child abuse and coercion and extortion of victims that have escalated in the last years;

- how to provide law enforcement with effective means to detect, investigate and bring down the many peer-to-peer networks and the growing number of forums on the darknet that facilitate the exchange of child sexual exploitation material and support offenders;
- how to help victims of abuse during criminal investigations and court procedures;
- how to help the victims in the long term, to help them deal with the effects;
- how to reduce risks of (re-)offending by better understanding the behaviour of abusers and potential abusers.

Sub-topic 2: [2019] Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour

The Internet of Things, the ever increasing number of internet-connected devices, may pose substantial threats to (cyber)security since this fully connected world as well as the network itself have become a target for cybercriminals. The key challenge in this respect is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated. The dissemination of "cybercrime-as-a-service" business models is an important enabler for crime and poses significant challenges to security. The increasing variety of such services, the modalities through which they are offered and the connections with different criminal activities need to be investigated to understand their trends and thus to allow for prevention and law enforcement.

Human factors determining online behaviour as described for instance by the online disinhibition effect (individuals acting more boldly online, being less inhibited and with their judgment impaired) are drivers for cybercrime as individuals feel disconnected from the actual crime or do not even perceive it as a crime. Recent trends also indicate a growth in cyber juvenile delinquency and a rise in adolescent hacking.

These developments call for further research in domains such as psychology, criminology, anthropology, neurobiology and cyber psychology to understand better the factors contributing to it and to devise preventive and deterrence measures, including providing alternatives to harness the potential of these young talents for cybersecurity and technologies.

- **Sub-topic 3: [2020] Developing evidence-based approaches to evaluate and to further develop initiatives to prevent and counter violent radicalisation**

The following issues are of particular interest: factors and pathways into radicalisation; factors influencing resilience to radicalisation, with a focus on groups requiring particular attention (such as children); the nexus between violent extremism and other forms of crime; violent extremism online (e.g., social media) and terrorist propaganda; evaluation and impact of counter-narratives and alternative narratives; how to address returnees, with a focus on children and women; dealing with extremists after their release from prison (and involving penitentiary services and legal authorities);gender and socio-economic aspects of radicalisation; challenges related to the lone actor phenomenon and evaluation of national and local prevent strategies. The objective of this sub-topic is not to support projects which cover

all those issues. Proposals should therefore address one or more of the issues mentioned above. They should take into account the importance of a multi-disciplinary, multi-agency and multi-stakeholder approach.

Proposals should refer to evidence-based research that compares and distils various approaches to the issue or issues that they are addressing, providing outcomes which are of direct use for policy makers and practitioners. Proposals should furthermore provide quantitative and/or qualitative indicators to allow for the evaluation of prevent, counter and de- radicalisation initiatives. The proposals could also analyse and evaluate different research methodologies in this field. Proposals should build on the expertise of different disciplines and stakeholders, including practitioners, in order to reflect the horizontal challenge of radicalisation.

The aim is not necessarily to develop new responses, but to focus on comparative analyses and evaluations of existing responses in order to identify transferrable and effective approaches based on what has been done so far, and/or to elaborate performance indicators and/or evaluation methods.

In line with the EU's strategy for international cooperation in research and innovation (COM(2012)492), international cooperation is encouraged.

If appropriate, the proposals should demonstrate how they will effectively build on relevant previous and on-going EU funded (including but not limited to the Internal Security Fund - Police) radicalisation projects.

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

Proposals analysing and recommending other ways to solve human, social, and societal 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, fundamental rights and applicable legislation, including in the area of privacy, protection of personal data and free movement of persons. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience, gender-related behaviours) 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 through multidisciplinary projects confronting different schools of thought. 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 EU Law Enforcement Agencies 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 EU Law Enforcement Agencies 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, cost-benefit considerations, as well as fundamental rights such as the rights to privacy, to protection of personal data and the free movement of persons;
- 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;
- advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals.

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 old, new and evolving 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. Novel robotized or automated tools for forensic analysis should be developed. 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.

Proposers are encouraged to address how they contribute to the European Forensic Science Area.[38]

- Sub-topic 2: [2018-2019] Digital forensics in the context of criminal investigations

New forensic tools, techniques 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, and enables investigations to identify perpetrators as well as victims, in particular in cases of child sexual abuses. They should focus on data gathering, data exploitation, and speedy exchange of information. All types of crime, terrorist activities and propaganda, and malicious acts by foreign-state perpetrators are concerned. Research in this domain should take into account new and emerging trends (for instance, abuse of encryption for criminal or terrorist purposes), while fully respecting fundamental rights such as the right to privacy and the right to protection of personal data.

In 2019, proposals should focus on data gathering, classification and exploitation, as well as speedy exchange of information in the context of child sexual abuses investigations, taking into account main and emerging trends (for instance, intensive use of Peer to Peer network, anonymous activity on the Dark Web and abuse of encryption).

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

Organized crime increasingly adopts technology (for example, pseudo-legal sales, shadow economy, internet/Darknet as well as cryptocurrencies) as a facilitator for preparation, organisation and execution of various physical/traditional criminal activities (e.g., child sexual abuse, trafficking of organs or human embryos, trafficking of human beings, trafficking of firearms, drug trafficking, money laundering and terrorism) and/or as a tool for online criminal activities (e.g., ransomware, domain-name piracy, phishing). Furthermore, there is a need for governing and detecting cross-border money flows with the potential to support terrorism, for reinforcing effective and legitimate public-private cooperation for the sharing of financial data, and for strengthening the effectiveness of current methods of countering terrorism financing and of modelling abnormal transactions in the fight against terrorism.

Research should address the following issues: approaches to identify new developments (new markets and networks; new modi operandi); tools for tracing money flows as well as those

[38] The Council Conclusions and the related Action Plan on the way forward in view of the creation of an European Forensic Science Area (EFSA) adopted on 9 June 2016: http://data.consilium.europa.eu/doc/document/ST-10128-2016-INIT/en/pdf.

engaged in criminal activities online whilst ensuring privacy and protection of personal data; Darknet marketplace analysis and mobility; tools for locating and mapping hidden service directories; tools for forensic analysis of digital media in order to identify digital currency datasets; data provenance models (providing evidence that is admissible in court), including the relationship between algorithmic proof artefacts and legal evidence.

- Sub-topic 4: [2020] Development and deployment of technologies, tools and relevant infrastructure to identify speedily terrorist content online, and prevent its re-upload

To address the threat of terrorist content online, the Commission has adopted a proposal for a Regulation on 12 September 2018.[39] Under the proposal a number of measures would be required to be taken by Member States (in particular law enforcement authorities)/Europol and hosting service providers. Hosting service providers from around the world (covering social media, cloud services, file sharing, etc.) offering their services to EU citizens would be required to put in place a certain number of measures, ranging from speedy reactive ones e.g. one hour deadline to remove or disable terrorist contents following a removal order from a Member State authority (considering that terrorist content is most harmful in the first hours of its appearance online) to proactive measures, including automated detection, in order effectively and swiftly to remove or to disable terrorist content and to stop it from reappearing and being disseminated once it has been removed.

Under the proposal, these measures would need to be implemented not only by large companies, but also by micro enterprises and SMEs, irrespective of size or turnover, albeit remaining proportionate. Putting in place such proactive/automated means is likely to create a burden on resources, hence mitigating measures for the benefit of smaller companies should be envisaged. Research should therefore be leveraged to support the development and deployment of technologies, tools and relevant infrastructure to identify speedily terrorist content online, and to prevent its re-upload. The media content analysis could play a relevant role in the development of tools for the active detection of harmful online behaviour (e.g. with natural language processing or image/video content analysis). The beneficiaries of such projects should include SMEs so as to ensure that the technology developed would be of direct relevance to their platforms. A further global take-up and dissemination of these technologies, tools and infrastructure where relevant should also be encouraged.

- 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; tracking and monitoring technologies, including automated prevention of uploading terrorism-related content; capabilities to detect the widest possible range of threats and concealments (including complex concealed weapons)) and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions).

[39] COM(2018) 640 final

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, fundamental rights and applicable legislation including in the area of privacy and protection of personal data. 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 in full compliance with applicable legislation on protection of personal data.

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 capabilities to improve the quality of data, and to convert voluminous and heterogeneous data sets (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) into actionable intelligence. These capabilities could be significantly enhanced 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, social network and darknet data analysis, and allow for resource-efficient, effective and proactive law enforcement.

Examples of trends in cybercrime are numerous. The Internet of Things can potentially connect practically everything, thus also potentially making everything more vulnerable. 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. Law Enforcement Agencies 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 patterns of abnormal behaviour. 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 techniques to allow for the identification of suspicious events or of criminals. 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 such as the right to privacy and the right to protection of personal data.

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 that both (a) characterise trends in cybercrime and in cybercriminal organizations (based on a profound analysis of current and emerging cybercriminal organizational types and structures), and (b) enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (stations, shopping malls, entertainment venues, etc.).

In 2020, proposals should address exclusively point b), with a focus on private operators. Although public authorities are primarily responsible for security, public-private cooperation is key in protecting public spaces. As an example, the first persons on the scene of a terrorist attack are often not police officers, but private security staff from local shops or transport operators. Moreover, public spaces are often owned and operated by private entities.

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation including in the area of privacy and protection of personal data. 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 Law Enforcement Agencies 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;
- improved capabilities to combine and analyse in near-real-time large volumes of heterogeneous data to anticipate criminal events;
- 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 amounts of data in the context of crowd protection in full compliance with applicable legislation on protection of personal data.

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: Chemicals: intelligence, detection, forensics

Specific Challenge: Criminals, including terrorists are constantly seeking new ways to develop, deploy and activate dangerous chemicals (explosives, neurotoxins, new drugs, etc.). The way in which such chemicals can be manufactured and combined evolve continuously, which makes the specialized work of law enforcement agencies (LEAs) and reference laboratories in this area a continuous challenge.

Scope: Research needs to anticipate and match this challenge by increasing the knowledge about these threats; developing technologies to counter and respond to incidents with them, improving knowledge on these dangerous chemicals and increasing deterrence messaging whilst also recognising the need to minimise the inconvenience that security measures place on operators and users of public spaces.

Proposals have to demonstrate how they will effectively build on relevant previous H2020 projects and build synergies with on-going H2020 projects.

Proposals should address only one of the following aspects:

- Proposals should focus on the continuation of the work already done on some explosive precursors in previous FP7 and H2020 projects, including; tackling new precursors not yet studied.

- Proposals should tackle the chemicals and potentially their precursors in the usage other than explosives and explosive precursors covered under the first point, and propose means to decrease the vulnerability of the public to their malevolent or terrorist use, along the full timeline of a potential criminal/terrorist plot (from early intelligence to the actual attack).

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 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: Short term:

- Improved knowledge of dangerous chemicals and of their combinations;

- Improved effectiveness of the supporting methods and techniques as well as of combinations of technologies used to prevent their use and to detect them before they are used;

- Improved mitigation methods, including designing strategies and forensic tools.

Medium/Long term:

- Contribution to improving public security;
- Factual scientific contribution to policy-makers in order to allow them to make an informed decision;
- Stronger involvement of practitioners in the field of counter-terrorist activities in making, assessing and selecting new tools and technologies through reliable management plans.
- Improving the training of law enforcement officers in this field and the cooperation at local, national and international level.

Type of Action: 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, on land and in the maritime domain. It contributes to the further development of the European Border Surveillance System (EUROSUR), its interoperability with other systems, and to enhance the 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, and migrant smuggling.

The aim of this section is to develop technologies and capabilities which are required to enhance systems and their interoperability, equipment, tools, processes, and methods for rapid identification to improve border security, whilst respecting fundamental rights including free movement of persons, protection of personal data, 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, law enforcement, 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 including gender. The adoption of appropriate organisational measures and the deeper understanding of how novel technologies and social media impact border control are required. 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. For the purpose of this topic, 'migration' does not refer to persons enjoying the right of free movement under Article 21 TFUE and secondary legislation (i.e. Union citizens and their family members, independently of their nationality).

Scope: Proposals (which should take into account already existing tools) 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 possibly resulting from certain perceptions abroad, that deviate from the reality of the EU

Research should investigate how to better detect and understand how the EU is perceived in countries abroad by analysing e.g. social media data, how such perception could possibly lead to threats and security issues on its citizens and territories, and how such perceptions can be avoided or even actively and effectively counteracted through various measures. 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.

- 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 and taking into account gender aspects, is required for high-level strategic decision-making, to plan and implement 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 propose convincingly how to better deal with such flows and to reduce risks of tensions and violence among migrants and European citizens.

Participation of Border or Coast Guards Authorities or those working with at-risk groups, for example first responders, municipalities, social workers, educators, civil society actors etc. is welcome.

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

EU border guards have to deal with diverse serious challenges at external borders, e.g. management of flows of people, smuggling and the use of counterfeit documents. Arrivals of thousands of people through one border area will quickly trigger a reaction, whereas the detections of a few cases of document fraud on a daily basis will be considered as part of the routine work and is unlikely to trigger a strong reaction. Research that assesses the impacts on the EU’s internal security of different threats and that proposes a model to compare those threats would assist in improving the situational awareness of decision-makers across the EU.

This research on external threats would also further enrich the vulnerability assessment tasks as defined in the European Border and Coast Guard Regulation.

Proposals should aim at improving the effectiveness of border control, including air, land and maritime borders, by developing dynamic composite indicators of threats, so that various threats occurring simultaneously at the border can be compared and priority for mitigation can be proposed. This should be based not only on the absolute number of detections at the border, but also on their synergies and inter-relationships, as well as on the impact that such detections may have on the internal security of the EU.

The fitness for purpose of the concepts proposed should be duly demonstrated in the relevant environment.

The Common Integrated Risk Assessment Model considers risk as a function of threat, vulnerability and impact. More information is available at: https://frontex.europa.eu/intelligence/ciram/.

More information on vulnerability assessment activities is available at: https://frontex.europa.eu/intelligence/vulnerability-assessment/.

- Sub-topic: [2018-2019] Open

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

Proposals should lead to solutions developed, tested and validated in compliance with European societal values, fundamental rights (including gender equality) and applicable legislation including in the area of free movement of persons, privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be analysed in a comprehensive and thorough manner with a view to facilitating future acceptance of such solutions.

Proposals should pursue truly innovative approaches. They should be submitted by consortia also involving civil society organisations. Synergies are encouraged with the work for the knowledge centre on migration 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, with fitness for purpose validated by policy-makers and by practitioners and in cooperation with civil-society

organisations in the Member States, the Associated Countries, and abroad where appropriate.

- 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, with fitness for purpose validated by practitioners and civil-society organisations.

- Advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals.

- [2020] Contribution to the development of EU joint capabilities for border management and support to the implementation of policy priorities

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 integrated situational awareness and applying augmented reality to border security

Currently, information is made available to border and coast guards in several formats and on different kinds of hardly interoperable displays. However, human cognitive is limited at managing information from several sources simultaneously and at handling too many separate pieces of equipment is a limit to their ability to act. Furthermore, border and coast guards often work in sparsely populated and remote areas where the availability of telecommunication networks may be an issue. Research and innovation should lead towards (cloud-based) integrated systems with simple but complete and highly-standardized interfaces showing real-time information in a user-friendly way that can assist border guards in decision-making, and in remaining in contact with their command and control centre in the actual context of operations. Water, land and air operating resources should be taken into account, to lead to enhanced concept of employment, integration and interoperability standards.

- 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. It is a cross-cutting priority according to the

EU Serious and Organised Crime Threat Assessment 2017[40], since it enables or enhances all types of serious and organized crime and terrorism. New countermeasures are needed to address potential frauds, in particular for the detection of morphed face images. The use of biometrics "on the fly" techniques for identification in a non-intrusive manner and without interrupting the flow of people is an area for further development, testing and validation.

- 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. To ensure security all along the "life cycle" of a voyage, new technologies can be implemented (together with methods for their deployment and possibly their integration into ship systems), as well as security novel procedures (including for embarkation and disembarkation, mooring at pier, etc.)

- Sub-topic 4: [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 should be facilitated by novel technologies and sensing strategies characterized by risk-based protection and non-intrusive security checks that can be implemented without disrupting business.

Proposals should target the automation and integration of existing technologies for the purpose of identifying the largest possible amount of threat materials and ensuring the full supervision of the logistic flow of goods. This would require exploiting information obtained through the analysis of cargo flow data available from open source and documentary control, intelligence gathering, risk management, as well as through physical detection or inspection of cargo in means of transport, luggage, or carried by individuals. The fitness for purpose of novel solutions should be validated at the EU external border, in a context chosen on the basis of a sound and factual risk analysis.

Of particular relevance: the enhancement of detection capabilities of contraband (mainly cigarettes) hidden in high density cargo (coal, iron ore) in particular for rail cargo transport, and well as the fight against illicit trafficking of radioactive and nuclear (NR) materials (including through the establishment of trans-European network of detection facilities with its specific concept of operations.

- Sub-topic 5: [2020] Disruptive technologies for non-intrusive identification of hidden goods

Detecting and identifying illegal goods hidden in containers, train cars and truck structures at EU external borders (e.g. ports, wharfs, rail yards, …) is a need shared by border guard, customs and law enforcement authorities. Illegal goods, including drugs, weapons, explosives, radiological and nuclear material, are trafficked into Europe by criminal organisations using a

[40] https://www.europol.europa.eu/socta/2017/

range of methods and tools, which are very diverse (e.g. to minimize the risk of detection during transportation, some drugs may be transformed into a liquid and turned back into a solid at destination) and adaptable to specific border conditions. These may also include taking advantage of new technology to facilitate access to containers.

Research should focus on the use of improved sensing technologies. The availability of a system of sensors producing a highly detailed, user friendly, 3-dimensional insight into the internal structure of a container (or truck), and the type of cargo carried, in a limited amount of time, would in particular be a valuable disruptive innovation for the customs and border inspection community. The system of sensors should be suitable for deployment and operation in a flexible and relocatable way, including mechanisms to improve field usability. The system should also allow for a swift gathering and exchange of information with other systems in order to facilitate a faster and more accurate localisation and identification of illicit cargo, without the need to open containers (this being a clear improvement when compared to current capabilities).

In line with the above, the newly developed solutions should allow for interoperability with state of the art and with foreseeable future border and customs information systems in order to optimise the overall container screening process using a risk-based approach.

Proposals should conduct testing and validation in the relevant environment.

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

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

Proposals should lead to solutions developed, tested, and validated in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. 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 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 progress is not deemed sufficient.

- 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 and in the future handbook for coast guards (as per Article 53 of the European Border and Coast Guard regulation.)

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;
- Implementation of the actions identified by the EU Strategy and Action Plan for customs risk management.

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

Specific Challenge: Solutions at high Technological Readiness Levels (TRL; please see General Annex G) to enhance border and external security do exist, but if they are not to remain unused they need to be demonstrated in the context of actual operations or exercises for validation by practitioners.

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 General Annex G.)

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

- Sub-topic 1: [2018] Remotely piloted aircrafts and underwater autonomous platforms to be used from on-board offshore patrol vessels

Remotely piloted autonomous platforms of all kinds should demonstrate innovative capacities for land border and coast surveillance. Underwater autonomous platforms are also of interest for choke points surveillance (i.e. a port entrance.)

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 wide 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 better situational awareness at the tactical level beyond coastal waters (up to 200 nautical miles), while reducing risks during search and rescue missions, including launch and recovery phases, even in adverse sea and weather conditions. 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 2: [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, including personal data. Innovative solutions are needed to ensure the interoperability of surveillance systems, and the availability of information for maritime border surveillance coming from the area of operations in standardized formats, 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 to incidents in the maritime domain, 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 3: [2020] Improved systems for the vessel tracking, behaviour analysis and automatic anomaly detection

Current maritime reporting systems (including ship reporting systems and container reporting systems) produce huge quantities of data which cannot be directly exploited by the human operators in the various maritime control centres. This is expected to be even more so in the near future, as the amount of data available shall increase with the introduction of VHF Data Exchange System (VDES). At the same time, non-homogenous sources of vessel information are accessible, these offer access to either open or proprietary data that could be used to perform risk analysis on each individual vessel navigating in, or on its way to, European waters.

Traditional reporting systems are not enough by themselves to allow for a reliable detection of anomalies. Therefore, research under this topic should focus on innovative solutions bringing together these three elements: reporting and surveillance systems data (e.g. containing information on a vessel journey), relevant information databases (containing vessels' and/or containers' historical information) and real or near real time data resulting from other reporting or surveillance sources. The aim is to provide more precise, more robust and earlier

anomaly detection. The combination of these sources of information should produce a risk scoring figure to be assigned to specific vessels which could, in turn, facilitate the discovery of possible illegal activities carried out by those vessels.

The solutions should be based on implementation agnostic, innovative algorithms for artificial intelligence and machine learning, applied to existing ship reporting systems and maritime databases and information sources. These algorithms should exploit, when appropriate and without precluding other methods, the capacity of Artificial Intelligence-enabled solutions. The solutions should automatically allocate risk level to vessels according to risk measured on the basis of anomalies detected on the reporting systems and on a vessel's previous history. Solutions should also take into account special requirements found when working with very large amounts of data, coming from a wide range of heterogeneous sources.

The fitness for purpose of the proposed solutions should be systematically tested and validated (i.e. planned, implemented, reported and assessed) in a real operational environment at the EU external borders under the control of potential end-users, delivering quantifiable, verifiable and comparable measures of effectiveness and performance. Proposals should recommend concrete approaches for their market uptake, taking into consideration the characteristics of the EU security market, business cases favourable for joint cross-border procurement and possible synergies with EU funding instruments.

Where appropriate, the use of CISE data and services model is encouraged. The research undertaken in previous projects (I2C, TRITON, MARISA..) should not be duplicated.

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

Proposals addressing other issues relevant to this challenge, based on a sound rationale and with the active involvement of a large number of relevant practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals submitted under this topic should be coordinated by a competent authority under civilian authority and command, nationally identified as specialised border or coast guard, or border police force.

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.*[41]

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, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data.

[41] https://ocean2020.eu/

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:

- 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 coast guard functions) 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.
- European standards for interoperable systems.
- Substantial and tangible improvement of (maritime) situational awareness and reaction capability, as appropriate in 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) and to its interoperability with other systems.
- [2020] Implementation of actions of civilian nature identified in the EU Maritime Security Strategy Action Plan.[42]

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):

[42] https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en

SU-GM01-2018-2019-2020: Pan-European networks of practitioners and other actors in the field of security[43]

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 3 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. 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. In 2019, proposals are invited to address the specific area of handling of hybrid threats in line with the existing EU policy framework.[44].

In 2020 proposals are invited to cover one of the two following options:

Option 1: security and intelligence services

The persistent terrorist threat is becoming increasingly diverse and complex. Emerging technologies add to the threat, but also provide opportunities. Security and intelligence services of EU Member States and Schengen partners are playing an important role to keep European citizens safe. European technological autonomy is particularly important in the field of intelligence. Intelligence and security services may have research needs that are different from law enforcement. Using tools based on cutting edge technology will be key to the performance of the services in the 21st century. Therefore, a network of practitioners from security and intelligence services of EU Member States, Associated Countries and, possibly, Schengen partners would be important to add this specific perspective to the identification of future research needs.

---

43 For 2018, 2019 and 2020 topics, this activity will be delegated to the Research Executive Agency, nevertheless the Commission reserves the possibility to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

44 The proposal should reflect the joint communication *Joint Framework on countering hybrid threats – a European Union response* (JOIN(2016) 18 final, 6 April 2016), while keeping in mind the *Guidance note — Research with an exclusive focus on civil applications*: http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf

Such a network could focus on interacting with relevant existing H2020 projects to provide input and feedback, on undertaking horizon scanning to identify emerging technologies and potential new threats and on identifying requirements for future research, which could include emerging technologies such as big data and artificial intelligence. In cooperation with the Commission, working methods would be identified to protect the specific requirements of the security and intelligence services participating in the consortium. The objective would be to support the needs of the security and intelligence services of the Member States, Associated Countries for future security research programming.

Option 2: fighting cybercrime

Several initiatives have been launched to identify existing gaps, and law enforcement authorities' needs in the area of cybercrime, to assess new threats and to develop roadmaps. This work has led to targeted research and development projects. However, in the area of cybercrime, technology and the threats scenarios evolve at such a pace that this work needs continuous updating. An accurate mapping of specific capacities in Member State authorities is still missing. Moreover, as cybercrime and crimes committed online happen without regard to borders it is necessary to identify as far as possible common challenges and solutions, so as to maximise the impact of available resources. As cybercrime investigations and digital forensics require specific expertise and tools (which are also needed for investigating crimes committed online in general), a dedicated network of practitioners, led by law enforcement experts, with a specific focus on cybercrime and more generally on the handling of digital evidence could therefore have a clear added value for assessing needs and gaps that can be tackled by capacity building including through research. In this context, the network could contribute to better prioritising and planning future EU funded research by: 1. Liaising with the relevant stakeholders in order to anticipate future capability needs and gaps in the field of fighting cybercrime; 2. Cataloguing, aggregating, processing and exploiting knowledge about current and future state of the art of technologies which can contribute to filling the capability gaps; 3. Communicating relevant findings to the relevant communities thus providing the required feedback to the research cycle, as well as to other technological capacity building initiatives launched at EU or national level.

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: 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**.**

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) and b);
- 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 the 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-GM02-2018-2020: Strategic pre-commercial procurements of innovative, advanced systems to support security[45]

Specific Challenge: Innovative solutions are needed when resources from different countries are required to work more closely together. Such solutions should support the development of the EU's Security Union.

Scope:

[45] For 2018, 2019 and 2020 topics, this activity will be delegated to the Research Executive Agency, nevertheless the Commission reserves the possibility to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

- **Sub-topic 1: [2018] Common requirements specifications for innovative, advanced systems to support security (CSA)**

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. Practitioner organisations may be private or public entities.

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.
- *Grants awarded under* this topic *will be complementary to the grant agreement under Sub-topic 2 of this Topic. The respective options of Article 2, and Article 41.4 of the Model Grant Agreement*[46] *will be applied.*

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

Proposals should lead to solutions to be developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. 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. All participating procurement authorities should also commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular with the principles of data protection by design and by default.

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

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.

Sub-topic 2: [2020] Procurement of prototype systems among those specified as a result of Sub-topic 1 (PCP)

The Commission invites practitioners involved in projects funded under Sub-topic 1 to submit proposals for this PCP stage based on requirements resulting from those projects.

Phase 1: To finalise the tendering documents package for a call for tenders to build security-relevant prototypes based on the technical input resulting from Sub-topic 1 of this Topic. To define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP stages;

Phase 2: To implement the call for tenders for research and development services. The call for tenders should envisage a competitive development composed of different stages that would lead to at least 2 prototypes from 2 different providers to be validated in real operational environment at the end of the PCP cycle;

Phase 3: To conduct the competitive development of the prototypes following the PCP principles including, at least, a design stage, an integration and technical verification stage and a validation in real environment stage. This process should be assessed following the procedures for verification and validation defined in the Phase 1;

Phase 4: To consolidate the results of the evaluation of the developed prototypes, extract conclusions and recommendations from the validation process, and to define a clear strategy for the further uptake of solutions. This strategy should consider joint-cross border procurement schemes and exploit synergies with other EU funds.

Proposals must build on the outcomes of the projects funded under Sub-topic 1. In order to guarantee a successful implementation of the PCP, proposals must provide clear evidence that such projects have delivered concrete outcomes on the following aspects:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;

- That there is a consolidated group of potential buyers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint-procurement of innovative solutions;

- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who would be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;

- That the state of the art and the market (including research) has been explored and mapped, and that there are different technical alternatives to address the proposed challenge;

- That the future PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready on due time in order to launch the call for the acquisition of R&D services according to the PCP rules.

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

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

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.

Proposals should ensure that solutions will be developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. 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. All participating procurement authorities should also commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular with the principles of data protection by design and by default.

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;

- Common solutions to address urgent security challenges jointly developed, integrated and valuated;
- Potential demand for security solutions, inspired by those developed, is aggrevated.

Medium term:

- To develop common technical specifications and reference performance levels for joint EU security solutions;
- To pave the road to market for technically mature and operationally relevant solutions and to accelerate their wide deployment in the EU.

Long Term:

- To contribute to narrowing down the gap between research and the market for the next generation of security solutions;
- To contribute to a single EU security market, by reducing market fragmentation and allowing exploitation of economies of scale;
- To facilitate access of new innovative players to the public procurement market;
- To contribute to reinforcing the competitiveness of the EU technology and industrial base.

Type of Action: Coordination and support action, Pre-Commercial Procurement

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

SU-GM03-2018: Pre-commercial procurements of innovative solutions to enhance security

Specific Challenge: Innovative solutions are needed when resources from different countries are required to work more closely together. Such solutions should support the development of the EU's Security Union.

Scope: Practitioners from several countries are invited to proceed with the procurement of innovative solutions to enhance their operational capability. Practitioner organisations may be private or public entities.

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, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. 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. All participating procurement authorities should also commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default.

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.
- High leveraging effect of the EU contribution to the action.

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):[47]

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	

[47] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

Opening: 15 Mar 2018				
SU-BES01-2018-2019-2020 (RIA)	10.00			28 Aug 2018
SU-BES02-2018-2019-2020 (RIA)	21.00			
SU-BES03-2018-2019-2020 (IA)	10.00			
SU-DRS01-2018-2019-2020 (RIA)	5.00			
SU-DRS02-2018-2019-2020 (RIA)	28.00			
SU-DRS03-2018-2019-2020 (IA)	6.00			
SU-FCT01-2018-2019-2020 (RIA)	10.00			
SU-FCT02-2018-2019-2020 (RIA)	21.00			
SU-FCT03-2018-2019-2020 (IA)	8.00			
SU-GM01-2018-2019-2020 (CSA)	5.00			
SU-GM02-2018-2020 (CSA)	6.00			
SU-GM03-2018 (PCP)	9.70			
Opening: 14 Mar 2019				
SU-BES01-2018-2019-2020 (RIA)		10.00		22 Aug 2019
SU-BES02-2018-2019-2020 (RIA)		21.00		
SU-BES03-2018-2019-2020 (IA)		10.00		
SU-DRS01-2018-2019-2020 (RIA)		5.00		
SU-DRS02-2018-2019-2020 (RIA)		28.20		
SU-DRS03-2018-2019-2020 (IA)		6.00		
SU-DRS04-2019-2020 (RIA)		10.50		
SU-DRS05-2019 (IA)		10.00		
SU-FCT01-2018-2019-2020 (RIA)		10.00		
SU-FCT02-2018-2019-2020 (RIA)		35.16		
SU-FCT03-2018-2019-2020 (IA)		8.00		
SU-GM01-2018-2019-2020 (CSA)		3.50		
Opening: 12 Mar 2020				

SU-BES01-2018-2019-2020 (RIA)			5.00	27 Aug 2020
SU-BES02-2018-2019-2020 (RIA)			21.00	
SU-BES03-2018-2019-2020 (IA)			10.00	
SU-DRS01-2018-2019-2020 (RIA)			5.00	
SU-DRS02-2018-2019-2020 (RIA)			21.00	
SU-DRS03-2018-2019-2020 (IA)			6.00	
SU-DRS04-2019-2020 (RIA)			7.00	
SU-FCT01-2018-2019-2020 (RIA)			10.00	
SU-FCT02-2018-2019-2020 (RIA)			27.20	
SU-FCT03-2018-2019-2020 (IA)			8.00	
SU-FCT04-2020 (IA)			10.00	
SU-GM01-2018-2019-2020 (CSA)			7.00	
SU-GM02-2018-2020 (PCP)			24.00	
Overall indicative budget	139.70	157.36	161.20	

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-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 5 such organisations, from at least 5 different EU or Associated

	countries. Topic "DRS03-2018-2019-2020, Sub-topic 2: [2019] Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)", requires the active involvement of at least 3 standardisation organisations from at least 3 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-DRS05-2019	This topic requires the active involvement of organizations in charge of national planning in relations with pandemics preparedness, from at least 5 different EU or Associated countries. This topic requires the active involvement of at least 3 first responder organizations, from at least 3 different EU or Associated countries. The duration of the proposed activity must not exceed 24 months.
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 5 such organisations, from at least 5 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. The duration of the proposed activities must not exceed 24 months.
SU-FCT04-2020	This topic requires the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or

	Associated countries. The duration of the proposed activities must not exceed 36 months.
SU-BES01-2018-2019-2020	In 2018 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 5 such organisations, from at least 5 different EU or Associated countries. In 2019 such conditions cease to apply. In 2020 predefined sub-topics require the active involvement of at least 3 Border Guards Authorities from at least 3 different EU or Associated countries.
SU-BES02-2018-2019-2020	In 2018 and 2019 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 5 such organisations, from at least 5 different EU or Associated countries. In 2020 predefined sub-topics require the active involvement of at least 3 Border Guards Authorities and/or Customs Authorities from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated countries.
SU-BES03-2018-2019-2020	In 2018 and 2019 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 5 such organisations, from at least 5 different EU or Associated countries. In 2020 predefined sub-topics require the active involvement of at least 3 Border Guards Authorities from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated countries.
SU-BES03-2018-2019-	Consortia must be coordinated by a practitioner organization

2020	under civilian authority and command. The duration of the proposed activities must not exceed 18 months.
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. 5. Only one network under each option may be supported. **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), and c) may be

	supported over the 2018-2019 period.
SU-GM02-2018-2020	In the Sub-topic called for in 2018 (Sub-topic 1), 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. In the Sub-topic called for in 2020 (Sub-topic 2), 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. Sub-topic 2 is only open to entities having successfully participated in actions under Sub-topic 1.
SU-GM03-2018	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 following exceptions apply:

SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-2018-2019-2020, SU-DRS02-2018-2019-2020, SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020, SU-GM01-2018-2019-2020	Grants will be awarded to proposals according to the ranking list. However, in order to ensure a balanced portfolio of supported actions, at least the highest-ranked proposal per sub-topic will be funded provided that it attains all thresholds.
SU-FCT04-2020	Grants will be awarded to proposals according to the ranking list. However, in order to ensure a balanced portfolio of supported actions, at least the highest-ranked proposal per aspect will be funded provided that it attains all thresholds.

The full evaluation procedure is described in the relevant guide published on the Funding & Tenders Portal.

Grant Conditions:

SU-BES03-2018-2019-2020	For grants awarded under this topic, the following cost categories will be ineligible costs: Cost of fuel The respective option of Article 6.5(c) [MSCA: 6.3] of the Model Grant Agreement will be applied.
SU-GM02-2018-2020	Under the Sub-topic called for in 2020 (Sub-topic 2) under this topic, the funding rate is 90% of the eligible costs. This rate is considered appropriate to give a strong incentive for PCPs in the areas identified under Sub-topic 1 under this topic while still maintaining a leverage effect by requiring a minimum contribution, albeit limited, from the participants.
SU-GM03-2018	Under this topic, the funding rate is 70% of the eligible costs. Given the broad openness of the topic, the amount invested by the buyers contributes to demonstrate their commitment and the interest in the outcome of the action.
SU-FCT03-2018-2019-2020, SU-GM02-2018-2020, SU-GM03-2018	For grants awarded under this topic the beneficiaries must grant access rights for EU institutions, bodies, offices or agencies and Member States under the special conditions for the Specific Objective 'Secure societies - Protecting freedom and security of Europe and its citizens'. The respective option of Article 31.5 of the Model Grant Agreement will be applied.
SU-GM02-2018-2020	Grants awarded under the Sub-topic called for in 2018 (Sub-topic 1) under this topic will be complementary to the following actions: the grant agreement under Sub-topic 2 of this Topic. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied.
SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-2018-2019-	For grants awarded under this Security call for Coordination and Support Actions, Pre-Commercial Procurement Actions, Innovation Actions and/or Research and Innovation Actions, the Commission or Agency may object to a transfer of ownership or

2020, SU-DRS01-2018-2019-2020, SU-DRS02-2018-2019-2020, SU-DRS03-2018-2019-2020, SU-DRS04-2019-2020, SU-DRS05-2019, SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020, SU-FCT03-2018-2019-2020, SU-FCT04-2020, SU-GM01-2018-2019-2020, SU-GM02-2018-2020, SU-GM03-2018	the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.
SU-DRS04-2019-2020	Option 1 of Article 41.3 of the Model Grant Agreement will be applied. Grants awarded under this topic will be complementary to the following action: 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 will be applied.

Consortium agreement:

SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-2018-2019-2020, SU-DRS01-2018-2019-2020, SU-DRS02-2018-2019-2020, SU-DRS03-2018-2019-2020, SU-DRS04-2019-2020, SU-DRS05-2019, SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020, SU-FCT03-2018-2019-2020, SU-FCT04-	Members of consortium are required to conclude a consortium agreement, in principle prior to the signature of the grant agreement.

2020, SU-GM01-2018-2019-2020, SU-GM02-2018-2020, SU-GM03-2018	

Call - Digital Security

H2020-SU-DS-2018-2019-2020

This Call deals with R&D and innovation towards enhancing digital security.

Proposals under this call should consider the relevant human factor and social aspects when developing innovative solutions. Where relevant, proposals should also describe how the gender dimension is taken into account in their content.

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[48]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

For grants awarded under these topics for Innovation Action and/or Research and Innovation Action, the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

All topics in this work programme part will be subject to security scrutiny.

Cybersecurity, Digital Privacy and data protection

The aim of this Call is to ensure society as a whole benefits from user-friendly systems on cybersecurity, digital privacy and personal data protection, enabling an active participation of citizens and organisations to their own security, privacy and personal data protection.

Trust and security are at the core of the Digital Single Market Strategy[49]*, while the fight against cybercrime is one of the three pillars of the European Agenda on Security*[50]*. The new set of measures in the area of cybersecurity building on previous actions has been recently announced in the Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"*[51].

48 http://eda.europa.eu/what-we-do/eda-priorities/research-technology
49 *Communication "A Digital Single Market Strategy for Europe" of 6.5.2015 - COM(2015) 192 final*
50 *Communication "The European Agenda on Security" of 28.4.2015 – COM (2015) 185 final*
51 *JOIN(2017) 450 final, Brussels, 13.9.2017*

The compliance of the European infrastructures, products and services with relevant directives (e.g. NIS [52] *, Data Protection Directive for Police and Criminal Justice Authorities*[53]*), regulations (e.g. eIDAS*[54]*, GDPR*[55]*, proposal for an e-Privacy regulation*[56]*) 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. Innovative solutions and services in digital security, privacy and personal data protection will open new market opportunities for the EU companies and will ensure a secure and trusted networked environment for the governments, businesses, individuals and smart things. Cybersecurity and privacy technologies will significantly contribute to strengthen the competitiveness of the EU industry and will enable its development as world leader in the global market.*

The Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry"[57] shaped the main related challenges and several strategic initiatives to address them. Established in July 2016, the contractual Public Private Partnership (cPPP) on Cybersecurity aims 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 for defining research and innovation priorities for 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 personal data protection common requirements. The topics below belonging to this Digital Security call are part of the contribution of the Commission to the Cybersecurity cPPP.

The European Commission has adopted a proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[58] to support the development of the technological and industrial capabilities necessary to autonomously secure its digital economy and increase Europe's competitiveness with regard to cybersecurity and privacy.

---

52 *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*

53 *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*

54 *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*

55 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

56 *Proposal for a Regulation of the European Parliament and of the Council - COM(2017) 10 final of 10.1.2017*

57 COM(2016) 410 final, Brussels, 5.7.2016

58 *COM(2018) 630,*

Proposals are invited against the following topic(s):

SU-DS01-2018: Cybersecurity preparedness - cyber range, simulation 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 and to make new security-related assumptions, identifying "zero-day" or potential unknown vulnerabilities, forecasting new threats (plus their cascading effects) and emerging attacks, and managing cyber risks.

Many organisations are unable to forecast and/or estimate the impacts of a cyber-risk. This results often in insufficient and/or irrelevant investments to ensure a more cyber secure environment. In addition, cybersecurity experts and professionals need to continuously adapt their expertise to a constantly evolving landscape with 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 competent cybersecurity professionals, 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.

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, digital privacy and personal data protection within the EU Digital Single Market.

Scope: 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 deliver 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, test and validate 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 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. Proposals should consider the specific needs of end-users, private and public security end-users alike. Proposals are encouraged to include public security end-users and/or private end-users, and to create operational links to the

Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs)[59] network across the EU.

Proposals should also develop, test and validate operational ways to continuously analyse the information collected by CERTs and/or CSIRTs and all relevant cybersecurity 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, and should also help in identifying the cost and time to recover following a cyber-attack.

In addition, the proposals should show that the econometric models contribute to: (i) identifying affordable security controls that are needed to protect valuable organization assets, (ii) promoting the development of cyber insurance and liability policies/contracts and (iii) fostering service level agreements addressing security, privacy and personal data protection requirements and policies. Proposals should bring innovative solutions to enforce and encourage accountability of security as a shared responsibility.

Proposals should also include (but should not be limited to) the delivery of solutions for specific social aspects of digital security related to training, in particular practical, operational and hands-on training, including: (i) increasing the dynamics of the training 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) integrating 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.

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 5 and 6 million would allow the specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

Short-term:

[59] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)

- 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, through cyber range and simulation;
- More organized collaboration between a network of cyber ranges and Europe-wide initiatives such as the CERTs/CSIRTs cooperation network of the NIS directive.
- Improved risks analysis models to be used by public/private organisations, through the use of economics for evidence-based cybersecurity and data privacy;
- Appropriate econometric models able to learn from cyber incident data on a wide scale;
- Improved knowledge on how organisations can make the right investment to secure their operations against cyber-attacks (e.g. where they result in personal data breaches[60]), using economics for evidence-based cybersecurity and data privacy;

Medium and long term:

- Improved resilience of ICT systems/infrastructures and reduced time and cost in infrastructures for training users;
- EU member states better prepared to face malware campaigns and to take down malicious infrastructures; improved EU-skills market;
- 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: Intelligent security and privacy management

Specific Challenge: In order to minimise security risks, ICT systems need to integrate state-of-the-art approaches for security and privacy management in a holistic and dynamic way. Organisations must constantly forecast, monitor and update the security of their ICT systems, relying as appropriate on Artificial Intelligence and automation, and reducing the level of human intervention necessary.

Security threats to complex ICT infrastructures, which are multi-tier and interconnected, computing architectures, can have multi-faceted and cascading effects. Addressing such

[60] Notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject are regulated under articles 33 and 34 of the GDPR.

threats requires organisations to collaborate and seamlessly share information related to security and privacy management.

The increasing prevalence and sophistication of the Internet of Things (IoT) and Artificial Intelligence (AI) broadens the attack surface and the risk of propagation. This calls for tools to automatically monitor and mitigate security risks, including those related to data and algorithms. Moreover, storage and processing of data in different interconnected places may increase the dependency on trusted third parties to coordinate transactions.

Advanced security and privacy management approaches include designing, developing and testing: (i) security/privacy management systems based on AI, including highly-automated analysis tools, and deceptive technology and counter-evasion techniques without necessary human involvement; (ii) AI-based static, dynamic and behaviour-based attack detection, information-hiding, deceptive and self-healing techniques; (iii) immersive and highly realistic, pattern-driven modelling and simulation tools, supporting computer-aided security design and evaluation, cybersecurity/privacy training and testing; and (iv) real-time, dynamic, accountable and secure trust, identity and access management in order to ensure secure and privacy-enabling interoperability of devices and systems.

Scope: Proposals are invited to address one of the sub-topics below. In addition, it would be an asset for proposals to include solutions for hands-on and state-of-the-art training, such as cybersecurity exercises.

Four pilot projects are launched under Horizon 2020 LEIT ICT, as a result of the call H2020-SU-ICT-2018, topic SU-ICT-03-2018 “Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap”. Proposals should therefore foresee actions to collaborate with these four projects and also with similar ongoing projects funded under H2020, and take account of the results and work done in other relevant H2020 projects on cybersecurity/privacy.

SME participation is strongly encouraged.

(a): Dynamic governance, risk management and compliance

Proposals should develop and integrate beyond state-of-the-art approaches to security and privacy management which are: automated, dynamic and adaptive, allowing to identify the vulnerabilities, threats, such as advanced persistent threats, and attacks (including zero-day attacks).

Proposals should include pilots with significant scale involving complex ICT systems and addressing several of the following: forecasting, risk-based situation awareness, evidence-based system and software assessment, visualisation techniques, real-time monitoring and alerts with high level of accuracy, support to fair automated decision-making, run-time adaptation and autonomous recovery from faulty states.

Proposals should address the technical, operational, financial and ethical dimensions of cybersecurity. Concrete application cases should be foreseen. Adapted tools, techniques and

formats for collaborative security/privacy event management and reporting should be proposed. Solutions involving advanced, highly representative simulation environments (cyber-ranges) might be proposed.

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.

Type of Action: Innovation Action

(b): Cyber-threat information sharing and analytics

Proposals should develop and test threat detection frameworks, which should to the extent possible include: (i) collaborative, open, and dynamic repositories of information on threats and vulnerabilities; (ii) build on and update existing ontologies, taxonomies and models; (iii) dynamic tools for automated detection with advanced analytic capabilities, and where possible response and recovery; (iv) accountability and audit techniques; and (v) synchronised real time self- encryption/decryption schemes with recovery capabilities.

Novel technologies enabling collaboration in cyber threat intelligence and alerting should be proposed, taking into consideration not only technical aspects, but also human aspects such as behavioural patterns, gender differences, privacy, ethics, sovereignty, psychology, linguistic and cultural boundaries.

The tools and services that will be developed should be in a position to support the operations of CERTs/CSIRTs and networks of CERTs/CSIRTs. Proposals should develop incident response tools and test respective processes for coordinated response to large-scale cross-border cybersecurity incidents and crises in line with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.[61]

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.

Type of Action: Innovation Action

(c): Advanced security and privacy solutions for end users or software developers

[61] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32017H1584

Proposals should develop automated tools for checking the security and privacy of data, systems, online services and applications, in view to support end users or software developers (possibly including developers of AI solutions) in their efforts to select, use and create trustworthy digital services. Proposals should address real application cases and at least one of the following services: automatic code generation, code and data auditing, trustworthy data boxes, forensics, certification and assurance, cyber insurance, cyber and AI ethics, and penetration testing.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 6; 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.

Type of Action: Research and Innovation Action

(d): Distributed trust management and digital identity solutions

With particular consideration to IoT contexts, applicants should propose and test/pilot innovative approaches addressing both of the following points: (i) distributed, dynamic and automated trust management and recovery solutions; and (ii) developing novel approaches to managing the identity of persons and/or objects, including self-encryption/decryption schemes with recovery ability. Proposals should address real application cases.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 5-6; 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 area to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Type of Action: Research and Innovation Action

Expected Impact:

In the short term, project outcomes should make relevant contributions to the following:

- reduced number and impact of cybersecurity incidents;
- efficient and low-cost implementation of the NIS Directive and General Data Protection Regulation;
- effective and timely co-operation and information sharing between and within organisations as well as self-recovery;
- availability of comprehensive, resource-efficient, and flexible security analytics and threat intelligence, keeping pace with new vulnerabilities and threats;

- availability of advanced tools and services to the CERTs/CSIRTs and networks of CERTs/CSIRTs;
- an EU industry better prepared for the threats to IoT, ICS (Industrial Control Systems), AI and other systems;
- self–recovering, interoperable, scalable, dynamic privacy-respecting identity management schemes.

In the medium to long term, project outcomes should make relevant contributions to the following:

- availability of better standardisation and automated assessment frameworks for secure networks and systems, allowing better-informed investment decisions related to security and privacy;
- availability and widespread adoption of distributed, enhanced trust management schemes including people and smart objects;
- availability of user-friendly and trustworthy on-line products, services and business;
- better preparedness against attacks on AI-based products and systems;
- a stronger, more innovative and more competitive EU cybersecurity industry, thus reducing dependence on technology imports;
- a more competitive offering of secure products and services by European providers in the Digital Single Market.

Type of Action: Innovation 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-DS03-2019-2020: 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 with cyber-attacks. The scale, value and sensitivity of personal data in the cyberspace are significantly increasing and citizens are typically uncertain about who monitors, accesses and modifies their personal data. Personal data breach may facilitate abuse by third parties, including cyber-threats such as coercion, extortion and corruption.

In order to protect the freedom, security and privacy, and ensure personal data protection of the citizens in Europe, citizens should be enabled to assess the risk involved in their digital activities and configure their own security, privacy and personal data protection settings and controls across these services. Citizens need to be fully aware that their informed consent is

necessary in many situations and become capable in providing their permission/consent for allowing accessing their personal data/devices/terminals with an increased level of granularity. Additionally there is a need for increased citizens' capacity to modulate the level and accuracy of the monitoring tools used by services (e.g. via cookies, positioning, tokens).

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 to large organizations. Security professionals and experts working for SMEs&MEs need to be in a constant learning 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 are invited against one of the following sub-topics:

(a): Protecting citizens' security, privacy and personal data

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

These solutions should include innovative approaches, techniques and user-friendly tools for: (1) improving resilience against privacy and personal data protection risks (e.g. personal data breaches[62]) and cyber threats (e.g. profiling, eavesdropping, data misuse); (2) identifying, removing and reporting potential harmful content (e.g. apology of criminal acts, unhealthy or self-harming habits) and abusive interactions (e.g. harassment, unsolicited communications); (3) exercising citizens' right to erasure ("right-to-be-forgotten")[63] and data portability[64]; (4) providing citizens with transparent information about their privacy and personal data protection[65] level and empowering them to modulate it at any moment of their digital activities (e.g. by activating encryption); (5) protecting or providing rights for any access/audit/interference with citizens' "smart terminals" or their Internet-based communications in a data protection compliant way; (6) developing on-line help-desks services or "one-stop-shop" informing, helping citizens in dealing with any security and/or privacy incident and data (including personal data) protection breach, and enabling them in reporting any cyber or privacy related incident and data (including personal data) protection breach. Such approaches need to build bridges/synergies with data protection authorities and CERTs/CSIRTs. To better respond to the needs and expectations of the end-users, proposals should engage the end-users by involving them in the design and implementation, in order to ensure the usability and acceptability of the proposed solutions. In addition, assurance and transparency about the digital security, privacy and personal data protection levels embedded

62 Notification off a personal data breach to the supervisory authority and communication of a personal data breach to the data subject are regulated respectively under articles 33 and 34 of the GDPR.
63 See article 17 of the GDPR.
64 See article 20 of the GDPR.
65 See article 12 of the GDPR.

in 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.

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 4 and 5 million would allow this specific challenge under sub-topic (a) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

Proposals should deliver innovative solutions 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 benefitting from innovative targeted solutions addressing their specific needs and available resources (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: (1) dynamically monitor, forecast and assess their security, privacy and personal data protection risks[66]; (2) become more aware of vulnerabilities, attacks and risks that influence their business; (3) manage and forecast their security, privacy and personal data protection risks in an easy and affordable way; (4) 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.

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 4 million would allow this specific challenge under sub-topic (b) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

[66] Data protection impact assessments are required in situation enumerated in article 35 of the GDPR.

- Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.

- Security, privacy and personal data protection are strengthened as 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 and data (including personal data) protection breaches.

- 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 and data breaches

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 advanced communications and interconnected systems, the EPES is increasingly exposed to external threats, such as worms, viruses, hackers and data privacy breaches.

Without appropriate cyber-defence measures, systems access could be violated (e.g. with the malware spreading over the system) and may cause power outages, damages and cascading effects to interconnected systems, and energy services. Therefore, with increased digitalisation, the EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk that allows taking proper countermeasures. For example, the growing use of interconnected smart devices in the EPES will increase the number of access points (e.g. smart meters, IoT), hence increasing the exposure to cyberattacks. In addition, even if security improvements may have been made since, legacy systems such as SCADA/ICS (Supervisory Control and Data Acquisition System/Industrial Control Systems) do not have cybersecurity measures embedded because designed in times when cybersecurity was not part of the technical specifications of the system design.

Furthermore, a control system in the EPES that is under attack might not be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts. On the other hand, with the decentralisation leading to a distributed energy system, microgrid operations and/or islanding could be further exploited against cyber-attacks and cascading effects in the EPES.

In order to pursue the integration of renewables and to ensure the benefits of a modern digitalised electricity grid, there is the need to detect and prevent threats with severe impacts and to shield the electric system against cyber-attacks. Without an adequate strategy and measures to protect the energy system from cyber-attacks, the energy transition would be more risky, more costly and possibly in danger.

The European Commission adopted in April 2019 a sector-specific guidance[67] that identifies the main actions required to preserve cybersecurity and be prepared to possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies. In March and April 2019 respectively, the European Parliament and the Council have adopted the proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"))[68].

Scope: The proposals should demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches (including personal data breaches) taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders. The proposals should 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 expected potential disruptive effects on the EPES should be envisaged and the relative counteracting measures should be designed, described, tested (sandboxing, simulations) on a representative energy demonstrator to verify effectiveness. Depending on the specific application, the proposal should 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 to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain); (ii) on that basis, designing adequate security measures to ensure a cyber-secure system and describing the advantages of the solutions adopted compared to others and which aim to guarantee the level of cybersecurity and resilience vital for EPES in an evolving system; (iii) implementing both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity; and (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis. The activities

[67] Recommendation C(2019)240 final and staff working document SWD(2019)1240 final

[68] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

may include the testing of micro-grid and/or islanding as a means to reduce the vulnerability to cyber-attacks.

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) define cybersecurity design principles with a set of common requirements to inherently secure EPES; (iii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and (iv) propose policy recommendations on EU exchange of information.

The dimension of pilots/demonstrators should be at large scale level (e.g. neighbourhood, city, regional level), involving generators, one primary substation, secondary substations and end users. The proposals are encouraged to 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.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020, in particular under the BRIDGE initiative[69].

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 amounts.

Expected Impact:

- Built/increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.
- Ensured continuity of the critical business energy operations and resilience against cyberattacks, including large scale, demonstrating effective solutions to a) the real-time constraints of an electric system, b) barriers to the cascading effect and c) the adaptation of legacy equipment or their coexistence with state of the art technology.
- The energy sector is better enabled to easily implement the NIS directive.
- A set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector will be made available.

[69] http://www.h2020-bridge.eu/

- Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector.

- Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.

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: Digital security, privacy, data protection and accountability in critical sectors

Specific Challenge: In critical vertical sectors/domains, cybersecurity technologies deployed in several application domains should be aligned to the specific domain needs, linking the demand and supply sides for such cyber technologies. In the context of an increased digitization and also of growing complexity of cyber-attacks, there are certain sectors/subsectors identified as critical from the point of view of cybersecurity needs in the NIS Directive: energy (electricity, oil, gas), transport (air transport, rail transport, water transport, road transport), banking, financial market infrastructures, health sector (health care settings, including hospitals and private clinics), drinking water supply and distribution, and digital infrastructure. 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 personal data protection. Building security, privacy and personal data protection by design and by default, principles and standards should be clearly defined to protect the critical infrastructures in these sectors and ensure personal data integrity and confidentiality.

For transport domain, 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, systems, entities and people. Personalized medicine is on the brink of becoming a successful approach in treating diseases. This increases the complexity of the pharmaceutical supply chain and raises the importance of achieving a zero error rate in the supply of personalized medications. Cybersecurity in this respect is safety critical and novel approaches are needed to ensure traceability and zero error deliveries. Moreover, requirements related to data protection

legislation should also be taken into account, as health is a very sensitive sector from this point of view[70].

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 and personal data protection of the people. Vulnerable patients' records management systems can be attacked leading to unauthorised disclosure of and access to personal data concerning health. Connected medical devices are increasingly used, in particular wearables and home health monitoring devices which often transmit sensitive data over unsecure wireless networks from the patients' home to the hospitals exposing the privacy and personal data of the patients and the resilience of the healthcare infrastructures.

Digital technologies are also profoundly changing the financial sector. Cybersecurity solutions are essential to make possible digital technologies for finance and for the stability of the financial sector which must respond to increasingly sophisticated cyber-attacks.

Scope: Among the critical sectors mentioned in the NIS Directive[71], proposals should treat generic aspects for at least two of them, by identifying common threats and attacks, and by developing proof of concepts for managing cybersecurity and privacy risks. In addition, proposals should treat specific aspects for one of the three critical sectors/domains mentioned as sub-topics, i.e. transport, healthcare and finance, by identifying specific vulnerabilities, propagation effects and counter measures, by developing and testing cyber innovation-based solutions and validating them in pilots/demonstrators. During the conception and development steps, critical sectors/domains' specificities, such as complexity of infrastructure and their large scale, should be taken into account. These pilots/demonstrators are encouraged to use relevant transversal cyber infrastructures and capabilities developed in other projects.

Proposals should also include (but should not be limited to) the delivery of specific social aspects of digital security related to training, in particular practical, operational and hands-on training, including: (i) increasing the dynamics of the training 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) integrating 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 against the following sub-topics below, in 2018 and 2019

(a) [2019]: Digital security, privacy and personal data protection in multimodal transport

[70] The GDPR in its Article 9 (processing of special categories of personal data) prohibits the processing of personal data concerning health unless one of the conditions set out in Article 9(2) apply.

[71] NIS directive - Annex II .

Proposals under this sub-topic should tackle on at least two of the following items:

(1): Secure access management for citizens to all types of vehicles. A European Single Transport market requires a pan-European, seamless privacy aware solution to access across mass, shared and individual mobility, which will bring added value to citizens while safeguarding data protection and privacy. However the corresponding increased interconnection of smarter systems increases the vulnerability surface and therefore novel tailored solutions should be proposed.

(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 delivered, 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, and personal data breaches in the multimodal transport service and operation. Proposals should improve the security intelligence of treating complex multimodal transport security and privacy incidents, notably personal data breaches, vulnerabilities and attacks. Proposals should develop practical solutions for relevant on-line sharing information and distributing real-time security, privacy and data protection warnings to all stakeholders in the multimodal transport ecosystem; collaboration with CERTs/CSIRTs is highly encouraged.

(3): Standardization to allow the quick adoption of cybersecurity best practices in the domain. Proposals should evaluate the feasibility of a security labelling for transport and deliver relevant recommendations and options.

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 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.

Type of Action: Innovation action

(b) [2019]: Digital security, privacy and personal data protection 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, data protection officers) of all entities in the healthcare ecosystem and considering all types of data handled, with special focus on sensitive data as defined by the GDPR.

Proposals under this sub-topic should tackle at least two of the following items:

(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 cybersecurity incident management systems.

(2): Deliver dynamic, evidence-based, sophisticated security, privacy and personal data protection 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).

(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 and personal data protection.

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 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.

Type of Action: Research and Innovation action

(c) [2018]: Digital security, privacy and personal data protection in finance

Proposals under this sub-topic should tackle at least one of the following items:

(1): Development of resilience enhancing technologies. Proposers are expected to develop innovative solutions tailored for 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 (i) deliver tools for making the exfiltration of data for attackers unattractive, both for ‘data at rest’ and 'data in transit'; (ii) consider incipient trends (e.g. digital on boarding based on biometric data); and (iii) collaborate with CERTs/CSIRTs.

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

(3): Standardization to allow the quick adoption of cybersecurity best practices in the domain. Applicants should propose novel solutions 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 4 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: Innovation action

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

Short term:

- 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.
- Identified relevant generic and specific aspects related to cybersecurity and digital privacy in the respective critical domains/sectors addressed.
- Advanced holistic systems and innovative proof concepts for managing cybersecurity and privacy risks in the respective critical domains/sectors addressed.
- Advances in the state-of-the-art analysis of specific aspects of the respective critical domains/sectors addressed, such as related cyber threats, attacks and vulnerabilities;
- Sound analysis of cascading effects of specific related cyber threats within the supply chain of the respective critical domains/sectors addressed.
- Improved cybersecurity information sharing and collaboration among stakeholders of the respective critical domains/sectors addressed, and with CERTs/CSIRTs.
- More targeted and acceptable security management solutions addressing specificities of the respective critical domains/sectors addressed.
- Trigger the fast adoption of cybersecurity/privacy/personal data protection best practices in the respective critical domains/sectors addressed.

Medium term:

- Better response and recovery technologies and services that will help organizations in the respective critical domains/sectors addressed to significantly reduce the impact of propagated and cascaded threats, vulnerabilities and breaches.
- Enhanced protection against emerging novel advanced threats in the respective critical sectors/domains addressed.
- Improved security governance of the respective critical domains/sectors addressed.
- Greater and more mature EU cybersecurity market in the respective critical domains/sectors addressed.
- Reduce the impact of breaches with various levels of success in penetrating the defences.

Long term:

- Better cybersecurity for specific standards in the respective critical domains/sectors addressed, that will trigger fast adoption of best practices in the related industry.
- Established trust chains among all entities in the eco-systems of the respective critical domains/sectors addressed.
- Better implementation of the relevant EU legislation (e.g. NIS, eIDAS, GDPR) in the respective critical domains/sectors addressed.
- Companies/organisations in the respective critical domains/sectors addressed are more willing to promote cyber security, privacy and personal data protection in the whole EU specific ecosystem.

Type of Action: Innovation action, Research and 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 - Digital Security

Opening date(s), deadline(s), indicative budget(s):[72]

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				

[72] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

SU-DS01-2018 (IA)	16.00			28 Aug 2018
SU-DS04-2018-2020 (IA)	20.00 [73]			
SU-DS05-2018-2019 (IA)	8.50			
Opening: 14 Mar 2019				
SU-DS03-2019-2020 (IA)		18.00		22 Aug 2019
SU-DS05-2018-2019 (RIA)		10.00		
SU-DS05-2018-2019 (IA)		10.00		
Opening: 12 Mar 2020				
SU-DS02-2020 (IA)			18.00	27 Aug 2020
SU-DS02-2020 (RIA)			20.00	
SU-DS03-2019-2020 (IA)			10.80	
SU-DS04-2018-2020 (IA)			20.00	
Overall indicative budget	44.50	38.00	68.80	

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. The following exceptions apply:

SU-DS02-2020, SU-DS03-2019-2020	Grants will be awarded to proposals according to the ranking list. However, for the 2020 topics only, in order to ensure a balanced portfolio of supported actions, at least the highest-

[73] of which EUR 5.00 million from the 'Secure, clean and efficient energy' WP part.

	ranked proposal per sub-topic will be funded provided that it attains all thresholds.

The full evaluation procedure is described in the relevant guide published on the Funding & Tenders Portal.

Consortium agreement:

All topics of this call	Members of consortium are required to conclude a consortium agreement prior to the signature of the grant agreement.

SME instrument & Fast-Track-to-Innovation

The respective calls for the EIC-SME instrument (H2020-EIC-SMEInst-2018-2020) and EIC-Fast-Track-to-Innovation (H2020-EIC-FTI-2018-2020) are found under the Horizon 2020 Work Programme Part – ***Towards the next EU Framework Programme for Research and Innovation: European Innovation Council (EIC) Pilot*** (part 17 of this work programme).

Other actions[74]

1. Reviews of projects

This action will support the use of appointed independent experts for the monitoring of actions (grant agreements, grant decisions, procurements, financial instruments).

Type of Action: Expert Contracts

Indicative budget: EUR 0.97 million from the 2018 budget (Review of projects) and EUR 0.74 million from the 2019 budget (Review of projects) and EUR 0.72 million from the 2020 budget (Review of projects)

2. Workshops, conferences, experts, communication activities, studies

- Organisation of an annual Security Research event.
- Support to workshops, expert groups, communications activities, or studies. Workshops are planned to be organised on various topics to involve end-users; preparation of information and communication materials, etc.
- 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 cybersecurity and digital privacy policy.

Type of Action: Public Procurement - Direct service contracts and specific contracts under framework contracts

Indicative timetable: First, second, third and fourth quarters of 2018, 2019 and 2020

Indicative budget: EUR 2.50 million from the 2018 budget and EUR 2.50 million from the 2019 budget and EUR 3.50 million from the 2020 budget (indicative number of contracts each year: 1 security research event, 2-4 workshop/communication activities/studies, 40-45 expert contracts, 3-5 in support to cybersecurity and/or digital privacy conferences/events/studies/policies/communication activities)

3. Space Surveillance and Tracking

Currently the space surveillance and tracking capabilities in Europe are fragmented and largely dependent on space surveillance systems controlled by third States. In order to ensure the protection of European infrastructure in space, as well as to move towards a greater autonomy of Europe in its access to and use of space, there is need for coordinated efforts at Union level in the field of SST, in particular in the areas of service provision, networking of assets and sensors.

[74] The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

The Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishes a Framework for Space Surveillance and Tracking Support (SST)[75].

The Consortium resulting from the implementation of the support framework for the emergence of an SST capacity at European level has established its own dedicated implementation structure in order to manage related Union support. Therefore support to SST under Horizon 2020 and other Union funding programmes should be entrusted to the above Consortium[76].

This activity consists in analysing, assessing and undertaking the necessary research, development and innovation activities with the specific aims of (1) supporting the pooling of national resources on the SST objectives outlined in the aforementioned Decision and coinciding with the Horizon 2020 objectives and challenges related to protecting Europe's investment made in space infrastructure; (2) supporting the upgrade and development of assets, including sensors, data processing, operating centres, network and infrastructure, and front desk, particular radars and telescopes, operated by Member States participating in the SST Support Framework in line with the EU overall Union SST research and development planarchitecture development roadmap; and (3) achieving significant economies of scale by joining related resources from Horizon 2020 (LEIT/space and secure societies), European Satellite Navigation Programmes and Copernicus, in addition to the cumulative national investment of the Member States participating in the SST support framework, which largely exceeds the Union contribution through the above Union funding programmes.

The aim is to improve the overall performance of the SST services and ensure, in the long-term, a high level of performance and appropriate autonomy at Union level. The activity should lead to a higher number of connected SST assets, allowing for improved quality and performance of SST in the future. Once these sensors have been networked and introduced in the operational Union SST chains, they will lead to a better orbital coverage and the collection of improved data, in terms of both quality and quantity. The integration of upgraded and developed sensors should be implemented in accordance with the needs for complementarity and optimisation of the SST architecture. This activity will also lead to closer interaction and complementarity among the various National Operations Centres and optimisation of the SST architecture thus achieving economies of scale while avoiding duplication.

This activity may involve the use of classified background information or the production of security sensitive foreground information. As such, certain deliverables may require security classification. The final decision on the classification of deliverables is subject to the security evaluation.

---

75 OJ L 158 of 27 May 2014, p. 227–234

76 In line with recital 24 of the Decision No 541/2014/EU, article 129 of the Financial Regulation (Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council) and article 193 of its Rules of Application (Commission Delegated Regulation (EU) No 1268/2012) this action may be financed jointly from separate source programmes, namely Horizon 2020 Framework Programme (Regulation (EU) No 1291/2013 of the European Parliament and of the Council), the Copernicus programme (Regulation (EU) No 377/2014 of the European Parliament and of the Council) and the European Satellite Navigation programmes (Regulation (EU) No 1285/2013 of the European Parliament and of the Council).

The activity will contribute to achieving the objectives set out in Annex 1 to the Commission Implementing Decision[77] on a coordination plan for the SST support framework and the procedure for participation of Member States[7879]. Impact will be assessed on the basis of the indicators and reporting obligations foreseen in the above Commission Implementing Decision.

The option of full purchase costs of equipment, infrastructure or other assets could be included in the GA if/when duly justified, in conformity of "Article 6.2 D.2" of the Horizon 2020 Model Grant Agreement.

This activity contributes to the Horizon 2020 focus area "Boosting the effectiveness of the Security Union ".

The identified beneficiary for this grant is the consortium resulting from the implementation of the SST support framework within the meaning of Article 7(3) of Decision No 541/2014/EU comprising entities designated by participating Member States[80],[81] and the EU SATCEN[82],[83]

Specific grant awarded under the Framework Partnership Agreement on Space Surveillance and Tracking for Research and Innovation Action. 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.

Type of Action: Specific Grant Agreement

Indicative timetable: Fourth quarter 2020

Indicative budget: EUR 3.00 million from the 2020 budget (EUR 3.00 million from the 2020 budget (Space Surveillance and Tracking))

77 COM(2016)8482 of 19.12.2016

78 http://ec.europa.eu/growth/sectors/space/security_en

79 In conjunction with the respective cumulative budget from Copernicus and EGNSS [and from H2020 Security

80 http://ec.europa.eu/growth/sectors/space/security_en

81 Article 195(d) of the Financial Regulation, Regulation (EU, Euratom) No 1046/2018 allows award of a grant without the call for proposals to "[…] bodies designated by the Members States, under their responsibility, where those Member States are identified by a basic act as beneficiaries of a grant".

82 Article 8 of Decision No 541/2014/EU: "*The European Union Satellite Centre (SATCEN) may cooperate with the consortium […]* ".

83 Article 195(f) of the Financial Regulation, Regulation (EU, Euratom) No 1046/2018 provides for an additional exception to calls for proposals " for activities with specific characteristics that require a particular type of body on account of its technical competence, its high degree of specialisation or its administrative powers, on condition that the activities concerned do not fall within the scope of a call for proposals''

4. Pre-standardisation mechanisms for security[84]

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

Pre-standardisation and standardisation processes as currently in place in the fields of security and civil protection are not considered satisfactory, whilst many of their components are very valuable: the JRC produces interesting pre-standards in cooperation with a broader research community; CEN/CENELEC and ETSI produce solid standards with the very active involvement of industry. However, both sets of activities are not very agile and they do not interface optimally.

These organizations are invited to propose mechanisms and novel ways of working and organizing themselves, towards the establishment of standardisation processes in the field of security that build upon the strength of the various processes in place, and increase their effectiveness, speed and efficiency.

Legal entities:

- Coordinator: European Committee for Standardization (CEN) - Brussels (Belgium)
- European Committee for Electrotechnical Standardization (CENELEC) - Brussels (Belgium)
- European Telecommunications Standards Institute (ETSI) - Valbonne (France)
- Joint Research Centre - Ispra (Italy)

This grant will be awarded without call for proposals in line with Article 190(1)(e) of the Rules of applications of Regulation (EU, Euratom) 966/2012, Regulation No 1268/2012 and Article 11(2) of the Rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)", Regulation (EU) No 1290/2013.

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

Indicative budget: EUR 0.90 million from the 2018 budget (Pre-standardisation mechanisms)

[84] This grant will be awarded without call for proposals in line with Article 190(1)(e) of the Rules of applications of Regulation (EU, Euratom) 966/2012, Regulation No 1268/2012 and Article 11(2) of the Rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)", Regulation (EU) No 1290/2013.

Budget[85]

	Budget line(s)	2018 Budget (EUR million)	2019 Budget (EUR million)	2020 Budget (EUR million)
Calls				
H2020-SU-INFRA-2018-2019-2020		24.00	38.00	15.00
	from 09.040303	*10.00*	*20.00*	*4.30*
	from 18.050301	*14.00*	*18.00*	*10.70*
H2020-SU-AI-2020				20.00
	from 09.040303			*5.70*
	from 18.050301			*14.30*
H2020-SU-SEC-2018-2019-2020		139.70	157.36	161.20
	from 18.050301	*139.70*	*157.36*	*161.20*
H2020-SU-DS-2018-2019-2020		39.50[86]	38.00	68.80
	from 09.040303	*39.50*	*38.00*	*68.80*
Contribution from this part to call H2020-EIC-FTI-2018-2020 under Part 17 of the work programme		3.87	3.87	3.87
	from 09.040303	*0.97*	*0.97*	*0.97*
	from 18.050301	*2.90*	*2.90*	*2.90*
Other actions				

85 The budget figures given in this table are rounded to two decimal places.
The budget amounts for the 2020 budget are subject to the availability of the appropriations provided for in the draft budget for 2020 after the adoption of the budget 2020 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.

86 To which EUR 5.00 million from the 'Secure, clean and efficient energy' WP part will be added making a total of EUR 44.50 million for this call.

Expert Contracts		0.97	0.74	0.72
	from 09.040303	*0.29*	*0.24*	*0.22*
	from 18.050301	*0.68*	*0.50*	*0.50*
Public Procurement		2.50	2.50	3.50
	from 18.050301	*2.00*	*2.00*	*3.00*
	from 09.040303	*0.50*	*0.50*	*0.50*
Specific Grant Agreement				3.00
	from 18.050301			*3.00*
Grant to Identified beneficiary		0.90		
	from 18.050301	*0.90*		
Estimated total budget		211.44	240.47	276.09