H2020 2018-2020 CALL SELECTION SC7 DRAFT WP

TOTAL CALLS	CODE	TOPIC/NAME	TYPE OF ACTION	TRL		BUDGET OF CALL	SUGGESTED PROJECT BUDGET	STAGE	OPENING DATE	DEADLINE
3				FROM	TO					
	SU-INFRA01	Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	IA		7	24	7-8	Single	15 Mar 2018	23 Aug 2018
			IA		7	22	7-8	Single	15 Mar 2020	27 Aug 2020
	SU-DRS03	Pre-normative research and demonstration for disaster-resilient societies	IA	6	7	6	6	Single	15 Mar 2018	23 Aug 2018
			IA	6	7	6	6	Single	15 Mar 2019	22 Aug 2019
			IA	6	7	6	6	Single	15 Mar 2020	27 Aug 2020
	SU-BES02	Technologies to enhance border and external security	RIA	4	6	21	7	Single	15 Mar 2018	23 Aug 2018
			RIA	4	6	21	7	Single	15 Mar 2019	22 Aug 2019
			RIA	4	6	21	7	Single	15 Mar 2020	27 Aug 2020

SU-INFRA01-2018-2019-2020: PREVENTION, DETECTION, RESPONSE AND MITIGATION OF COMBINED PHYSICAL AND CYBER THREATS TO CRITICAL INFRASTRUCTURE IN EUROPE

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) address in detail all aspects of interdependent physical (e.g. bombing, sabotage and attacks with a variety of weapons against installations and buildings, 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, and

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

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), 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. Priorities for 2020 will be defined at a later stage. When selecting for funding the proposals submitted in 2018 or 2019, the Commission will take due account of similar projects financed 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 participant 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.

SU-DRS03-2018-2019-2020: PRE-NORMATIVE RESEARCH AND DEMONSTRATION FOR DISASTER- RESILIENT SOCIETIES

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

SU-BES02-2018-2019-2020: TECHNOLOGIES TO ENHANCE BORDER AND EXTERNAL SECURITY

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 employement, integration and interoperability standards.