ISERD
המינהלת הישראלית למו"פ האירופי
Israel-Europe R&I Directorate

HORIZON2020
Secure Societies Information Day

2019 SEC Topics

02.04.2019

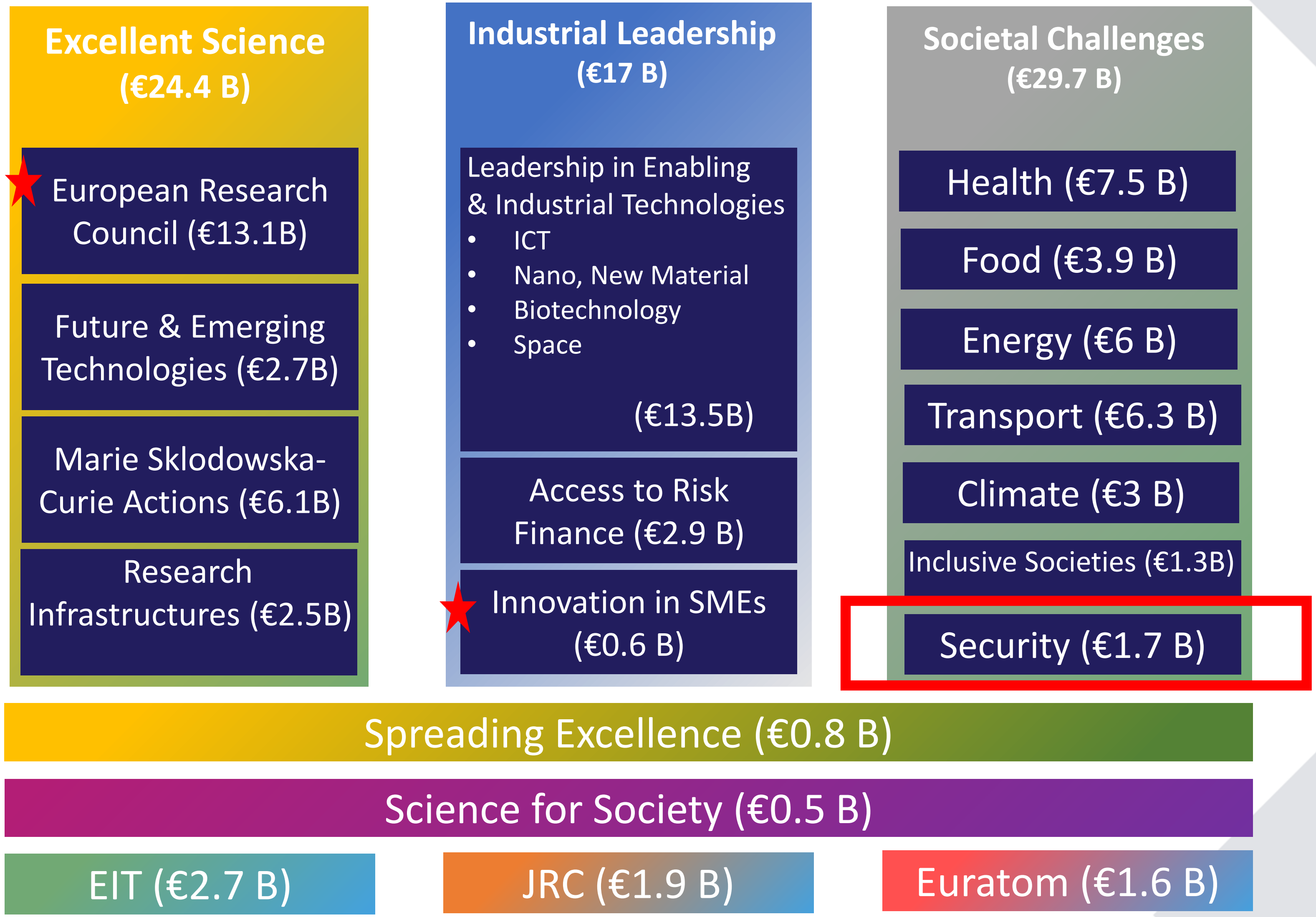
Talia Passiar
Secure Societies National Contact Point (NCP)

רשות החדשנות
Israel Innovation Authority

Ministry of Science
Technology & Space

המועצה להשכלה גבוהה
COUNCIL FOR HIGHER EDUCATION
ועדה לתכנון ולתקצוב
PLANING & BUDGETING COMMITTEE

Horizon 2020



Excellent Science (€24.4 B)

- ★ European Research Council (€13.1B)
- Future & Emerging Technologies (€2.7B)
- Marie Sklodowska-Curie Actions (€6.1B)
- Research Infrastructures (€2.5B)

Industrial Leadership (€17 B)

- Leadership in Enabling & Industrial Technologies
  - ICT
  - Nano, New Material
  - Biotechnology
  - Space

  (€13.5B)
- Access to Risk Finance (€2.9 B)
- ★ Innovation in SMEs (€0.6 B)

Societal Challenges (€29.7 B)

- Health (€7.5 B)
- Food (€3.9 B)
- Energy (€6 B)
- Transport (€6.3 B)
- Climate (€3 B)
- Inclusive Societies (€1.3B)
- Security (€1.7 B)

Spreading Excellence (€0.8 B)

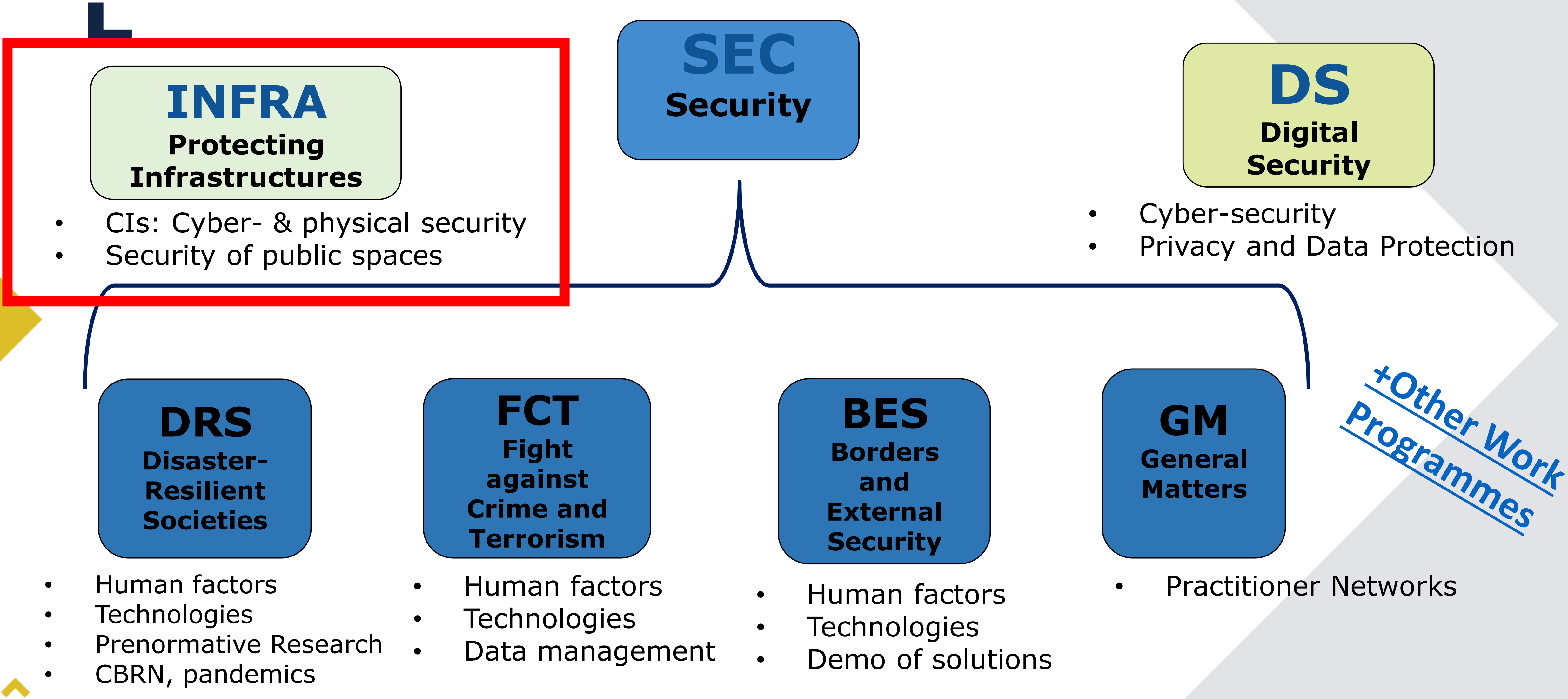
Science for Society (€0.5 B)

EIT (€2.7 B)

JRC (€1.9 B)

Euratom (€1.6 B)

Work Programme 2018-2020 - Structure



SEC
Security

INFRA
Protecting Infrastructures

- CIs: Cyber- & physical security
- Security of public spaces

DRS
Disaster-Resilient Societies

- Human factors
- Technologies
- Prenormative Research
- CBRN, pandemics

FCT
Fight against Crime and Terrorism

- Human factors
- Technologies
- Data management

BES
Borders and External Security

- Human factors
- Technologies
- Demo of solutions

GM
General Matters

- Practitioner Networks

DS
Digital Security

- Cyber-security
- Privacy and Data Protection

+Other Work Programmes

Critical Infrastructure Protection (INFRA)

Area	Topic	Budget (M€)	Funding Terms
Protecting the infrastructure of Europe and the people in the European smart cities	SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	**2019**: 22.00	IA - 70% €7-8M per project

Conditions –

- TRL 7 (prototype demo in operational environment)
- At least 2 operators of the chosen type of critical infrastructure from 2 MS or AC
- Industry involvement is mandatory
- SME participation encouraged
- International cooperation encouraged (especially with IFAFRI)
- Up to 24 months duration

Technical Aspects: SU-INFRA01-2018-2019-2020

Water systems

Energy infrastructure (Energy value chain, Gas networks, **Others**)

Transport infrastructure (Ports, Airports, **Others**)

Communication infrastructure

Ground segments of space systems

Health services

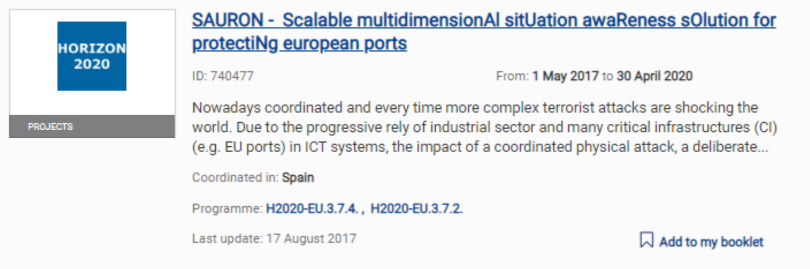
E-Commerce and postal infrastructure

Sensitive industrial sites and plants

Financial services

*Areas in black, , covered in calls 2016 and 2017
**Areas in green, to be covered following 2018 evaluation
*****Areas in Red not yet covered**

Previously Funded Projects



SAURON - Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports

ID: 740477 From: 1 May 2017 to 30 April 2020

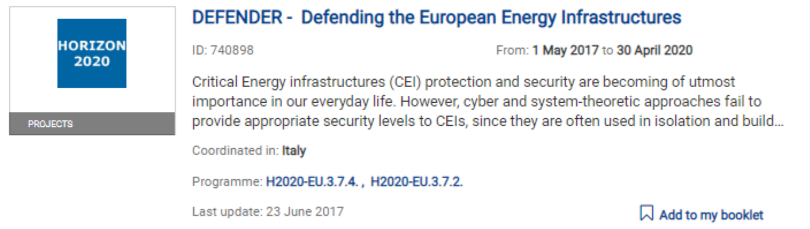
Nowadays coordinated and every time more complex terrorist attacks are shocking the world. Due to the progressive rely of industrial sector and many critical infrastructures (CI) (e.g. EU ports) in ICT systems, the impact of a coordinated physical attack, a deliberate...

Coordinated in: Spain

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 17 August 2017

Add to my booklet



DEFENDER - Defending the European Energy Infrastructures

ID: 740898 From: 1 May 2017 to 30 April 2020

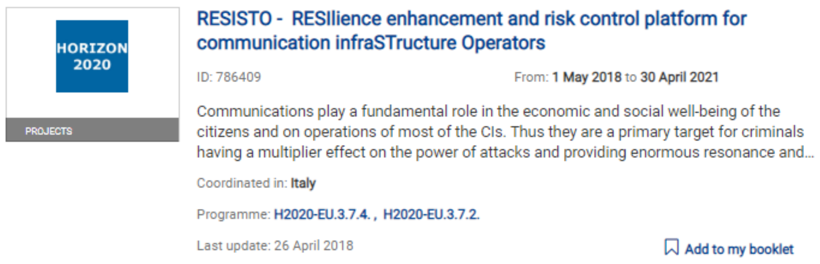
Critical Energy infrastructures (CEI) protection and security are becoming of utmost importance in our everyday life. However, cyber and system-theoretic approaches fail to provide appropriate security levels to CEIs, since they are often used in isolation and build...

Coordinated in: Italy

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 23 June 2017

Add to my booklet



RESISTO - RESIlience enhancement and risk control platform for communication infraSTructure Operators

ID: 786409 From: 1 May 2018 to 30 April 2021

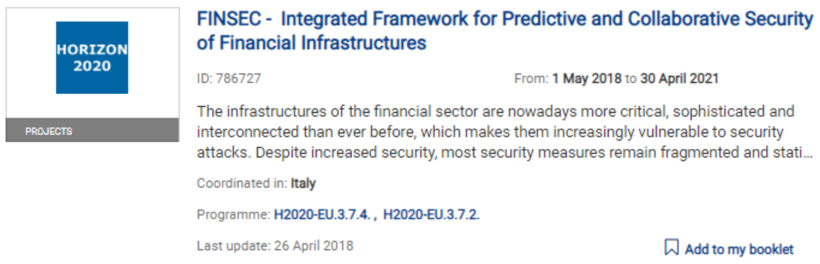
Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and...

Coordinated in: Italy

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 26 April 2018

Add to my booklet



FINSEC - Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures

ID: 786727 From: 1 May 2018 to 30 April 2021

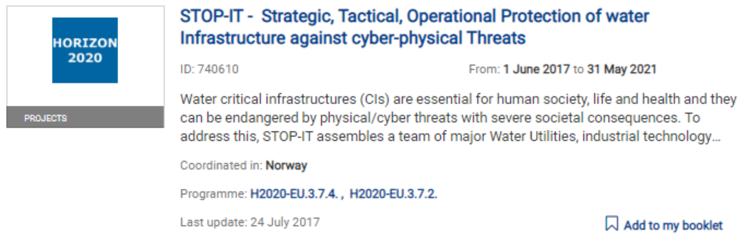
The infrastructures of the financial sector are nowadays more critical, sophisticated and interconnected than ever before, which makes them increasingly vulnerable to security attacks. Despite increased security, most security measures remain fragmented and stati...

Coordinated in: Italy

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 26 April 2018

Add to my booklet



STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

ID: 740610 From: 1 June 2017 to 31 May 2021

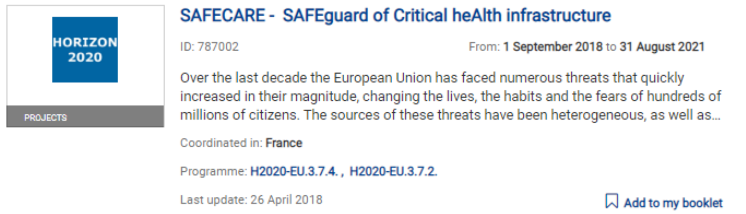
Water critical infrastructures (CIs) are essential for human society, life and health and they can be endangered by physical/cyber threats with severe societal consequences. To address this, STOP-IT assembles a team of major Water Utilities, industrial technology...

Coordinated in: Norway

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 24 July 2017

Add to my booklet



SAFECARE - SAFEguard of Critical heAlth infrastructure

ID: 787002 From: 1 September 2018 to 31 August 2021

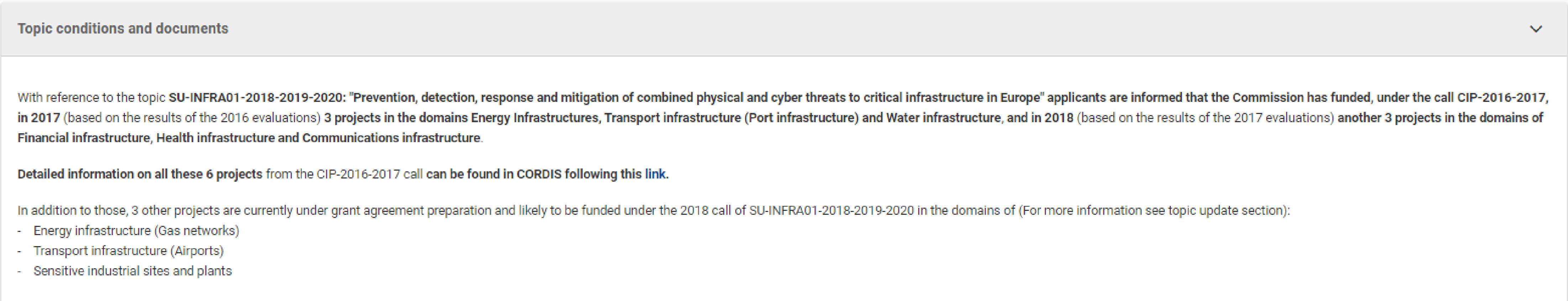
Over the last decade the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as...

Coordinated in: France

Programme: H2020-EU.3.7.4. , H2020-EU.3.7.2.

Last update: 26 April 2018

Add to my booklet



Topic conditions and documents

With reference to the topic **SU-INFRA01-2018-2019-2020: "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe" applicants are informed that the Commission has funded, under the call CIP-2016-2017, in 2017** (based on the results of the 2016 evaluations) **3 projects in the domains Energy Infrastructures, Transport infrastructure (Port infrastructure) and Water infrastructure, and in 2018** (based on the results of the 2017 evaluations) **another 3 projects in the domains of Financial infrastructure, Health infrastructure and Communications infrastructure**.

Detailed information on all these 6 projects from the CIP-2016-2017 call **can be found in CORDIS following this link.**

In addition to those, 3 other projects are currently under grant agreement preparation and likely to be funded under the 2018 call of SU-INFRA01-2018-2019-2020 in the domains of (For more information see topic update section):
- Energy infrastructure (Gas networks)
- Transport infrastructure (Airports)
- Sensitive industrial sites and plants

Critical Infrastructure Protection (INFRA)

Area	Topic	Budget (M€)	Funding Terms
Protecting the infrastructure of Europe and the people in the European smart cities	SU-INFRA02-2019: Security for smart and safe cities, including for public spaces. Develop and integrate experimentally, components of an open platform for sharing and managing information between public service operators and security practitioners of a large, smart city	**2019**: 16.00	IA - 70% €8M per project

Conditions –

- TRL 7 (prototype demo in operational environment)
- At least 2 local city/metropolitan governments from 2 MS or AC
- Industry involvement is mandatory
- Involvement of public and private operators (shopping malls, sport and transport venues…)
- Synergies with UIA (Urban Innovation Actions)
- Up to 24 months duration

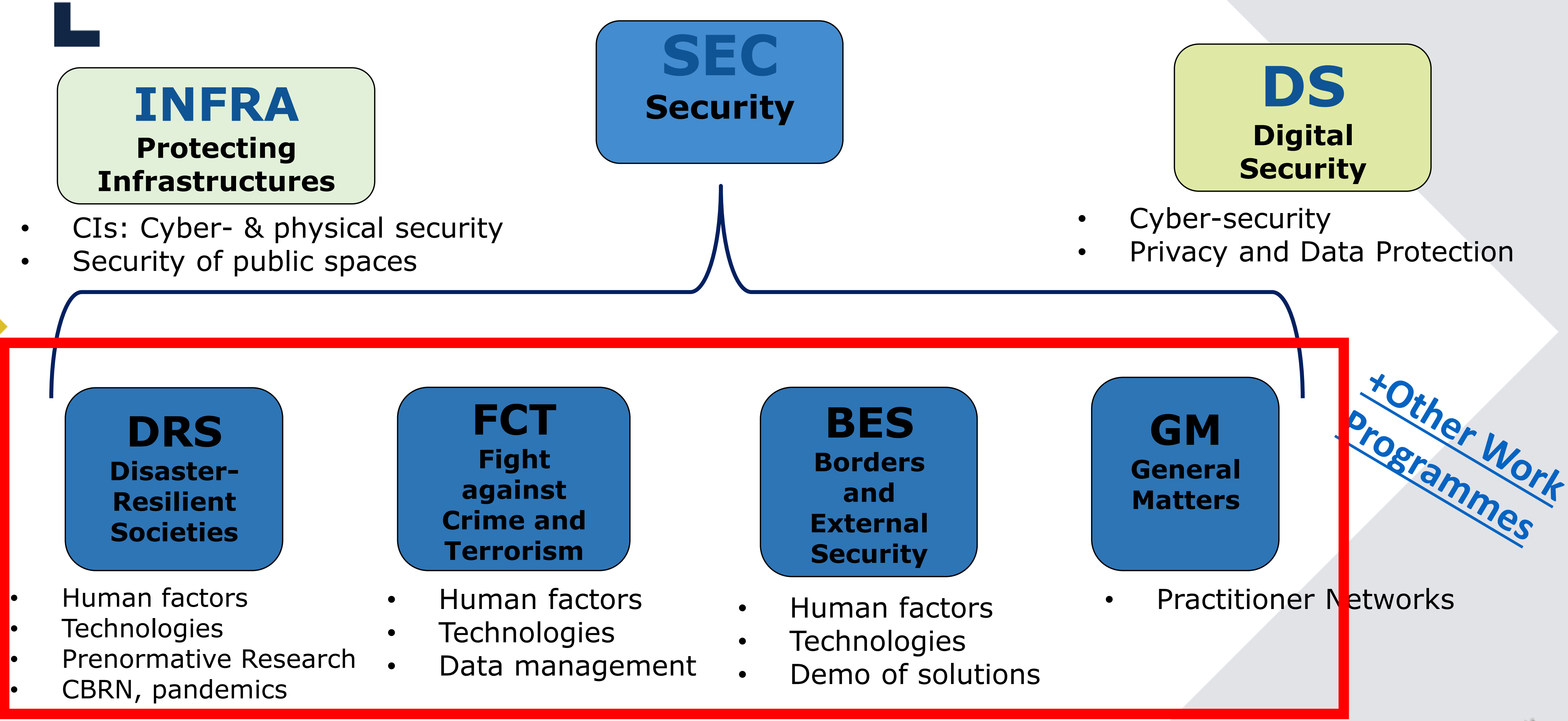
Policy Documents

- Good practices to support the protection of public spaces
- Identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- A European Programme for Critical Infrastructure Protection
- Seventeenth Progress Report towards an effective and genuine Security Union
- Action Plan to support the protection of public spaces

Main Priorities

- Identification of tools, including indicators, to protect CIs from Hybrid Threats;
- Methods and tools for addressing insider threats to CI, such as background checks and awareness raising in cooperation with relevant authorities;
- New challenges to CIP and emerging threats (e.g. drones…)
- Other: CI Risk assessment methods, transnational cooperation, civilian-military cooperation / cooperation with international organisations

Work Programme 2018-2020 - Structure



SEC
Security

INFRA
Protecting Infrastructures

- CIs: Cyber- & physical security
- Security of public spaces

DS
Digital Security

- Cyber-security
- Privacy and Data Protection

DRS
Disaster-Resilient Societies

- Human factors
- Technologies
- Prenormative Research
- CBRN, pandemics

FCT
Fight against Crime and Terrorism

- Human factors
- Technologies
- Data management

BES
Borders and External Security

- Human factors
- Technologies
- Demo of solutions

GM
General Matters

- Practitioner Networks

+Other Work Programmes

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS01-2018-2019-2020: Human factors, and social, societal, and organisational aspects for disaster-resilient societies	**2019**: 5.00	RIA - 100% €5M per project

Conditions –

- Active involvement of at least 3 first responders' organisations or agencies from at least 3 different EU or Associated countries
- International cooperation encouraged but not mandatory
- Risk awareness, risk management, and risk perception should be addressed
- Diversity of disasters as well as social media or crowd sourcing data in emergency situations can be explained

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS01-2018-2019-2020: Human factors, and social, societal, and organizational aspects for disaster-resilient societies	**2019**: 5.00	RIA - 100% €5M per project

Previously funded –

- Understanding how the most vulnerable segments of population are exposed to disasters, to provide recommendations for stakeholders on the use of social media and to engage them in the co-creation and evaluation of policies, strategies and tools.
- Understanding resilience in societies and local communities, to innovate on the strategies and solutions for improving resilience and to communicate, demonstrate and assess the validity of the project outcomes

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS02-2018-2019-2020: Technologies for first responders **[sub-topic 2] - 2019** - Innovation for rapid and accurate pathogens detection **[sub-topic 4] - 2018 – 2019 - 2020** – Open	**2019**: 21.00	RIA - 100% €7M per project

Conditions –

- TRL 4-6 (technology validated in lab - prototype demonstrated in relevant environment)
- Active involvement of at least 3 agencies or first responders' organisations from at least 3 different EU or Associated countries
- Open requires the active involvement of at least 5 such organisations
- International cooperation is encouraged (but not mandatory), in particular with Japanese or Korean research centers
- Open does not have to address a large scale scenario or have multidisciplinary first responders

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS02-2018-2019-2020: Technologies for first responders **[sub-topic 2] - 2019** - Innovation for rapid and accurate pathogens detection **[sub-topic 4] - 2018 – 2019 - 2020** – Open	**2019**: 21.00	RIA - 100% €7M per project

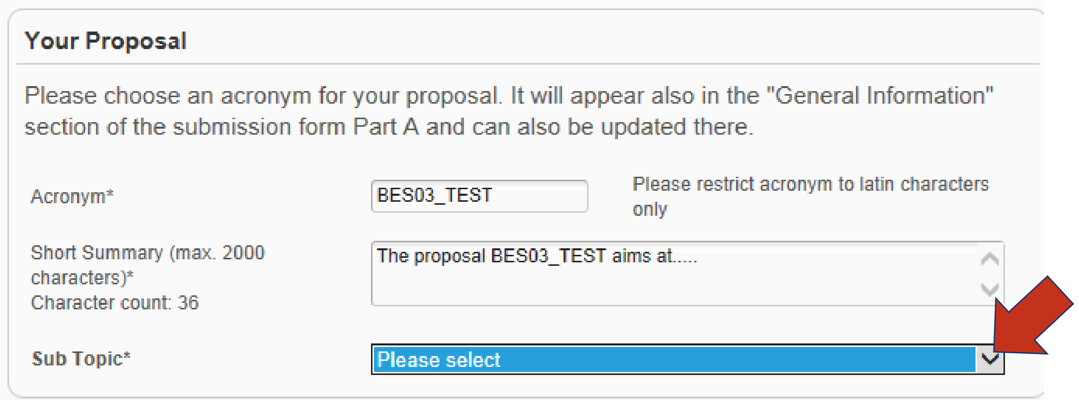
Previously funded (open) –

- Validated solutions addressing the protection of first responders in hazardous environments
- Improved capabilities and skills of First Responders organisations with a focus on their cooperative work during the mitigation of large disasters
- A Next Generation Integrated Toolkit (NGIT) for collaborative response
- Integrated multi-drone emergency solution with fieldproven procedures that will be integrated it into the current first responders' operational workflow.

Mandatory sub-topic selection (for SEC only)

- Only applicable to 6 topics (≥ open 2 sub-topics in 2019):

  BES01, BES02, BES03, DRS02, FCT01, FCT02

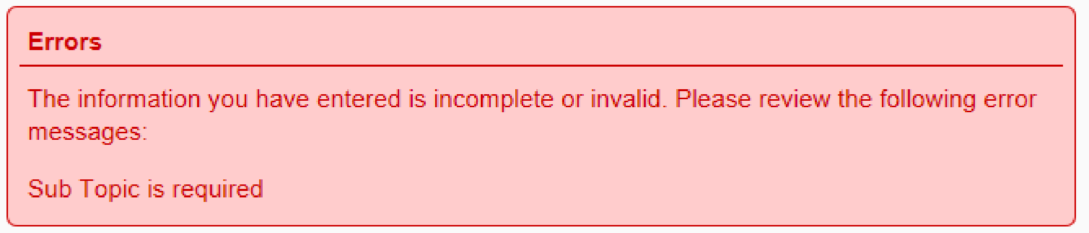


Your Proposal

Please choose an acronym for your proposal. It will appear also in the "General Information" section of the submission form Part A and can also be updated there.

Acronym*	BES03_TEST	Please restrict acronym to latin characters only
Short Summary (max. 2000 characters)* Character count: 36	The proposal BES03_TEST aims at.....	
Sub Topic*	Please select	

- Sub-topic selection required (blocking feature):



Errors

The information you have entered is incomplete or invalid. Please review the following error messages:

Sub Topic is required

- Sub-topic *visible in part A* and *can* be changed later

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS03-2018-2019-2020: Pre-normative research and demonstration for disaster resilient societies **[sub-topic 2] - 2019** – Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)	2019: 6.00	IA - 70% €6M per project

Conditions –

- TRL 6-7 (technology/prototype demonstrated in relevant environment)
- Active involvement of at least 3 agencies or first responders' organisations from at least 3 different EU or Associated countries
- It is recommended to check ResiSTAND recommendations

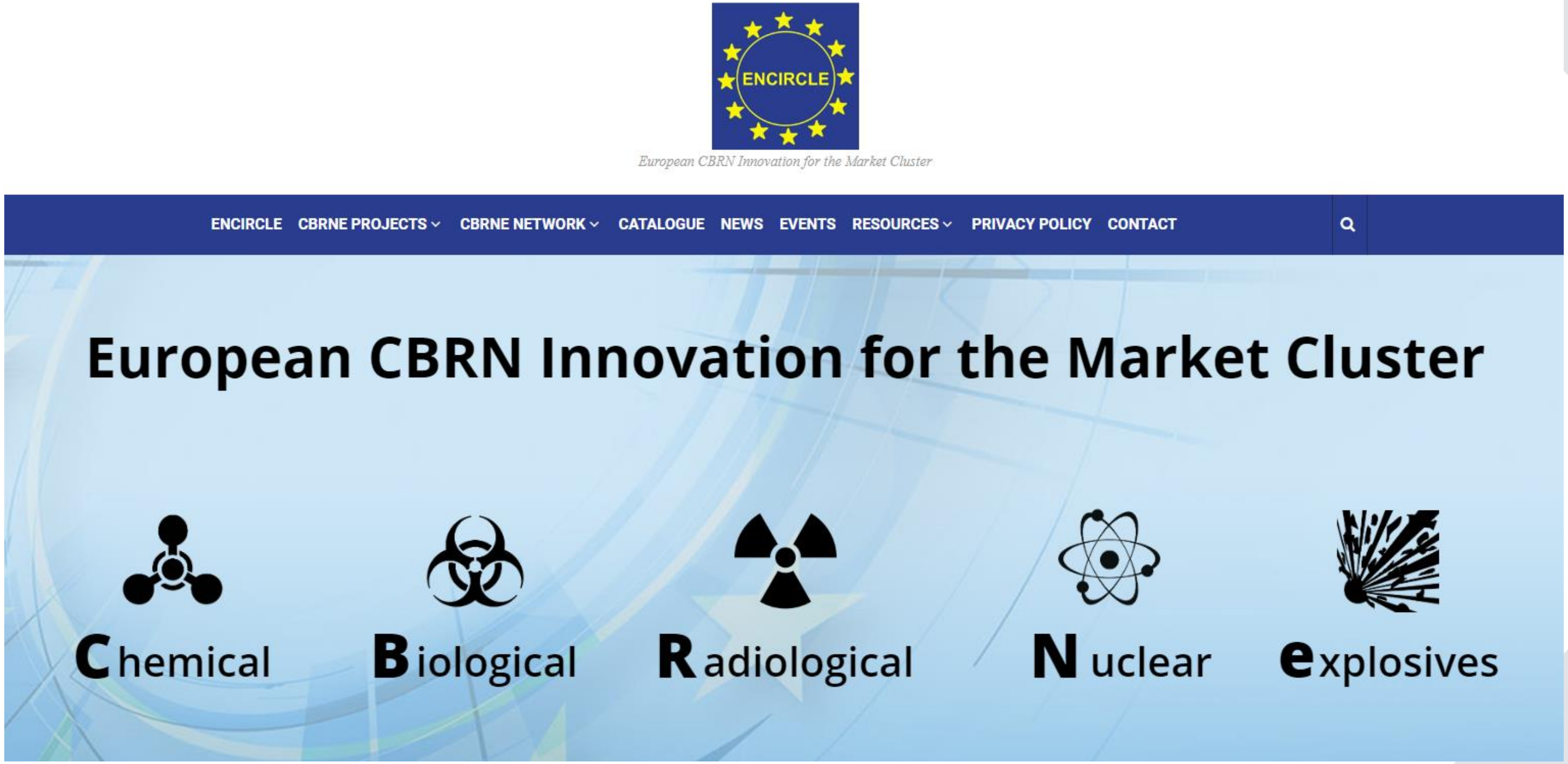
Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS04-2019-2020: Chemical, biological, radiological and nuclear (CBRN) cluster	2019: 10.50	RIA - 100% €3.5M per project

Conditions –

- Establish a "Collaboration Agreement" with participant(s) in the ENCIRCLE consortium
- Coordinator must be an SME
- TRL 4-6 (technology/prototype demonstrated in relevant environment)

Previously Funded Projects



ENCIRCLE

European CBRN Innovation for the Market Cluster

European CBRN Innovation for the Market Cluster

It is mandatory to address capability gaps presented by ENCIRCLE

Disaster Resilience - DRS

Area	Topic	Budget (M€)	Funding Terms
Disaster Resilient Societies (DRS)	SU-DRS05-2019: Demonstration of novel concepts for the management of pandemic crises	2019: 10.00	IA - 70% €10M per project

Conditions –

- Active involvement of organizations in charge of national planning in relations with pandemics preparedness, from at least 5 different EU or Associated countries
- Active involvement of at least 3 first responder organizations, from at least 3 different EU or Associated countries
- Up to 24 months

Policy Documents

Disaster Resilient Society

DG HOME
Internal Security

CBRN Action Plan
+CBRN-E risks
+ European Agenda on Security

DG ECHO
Civil Protection

EU Civil Protection Mechanism

DG GROW
Enterprise & Industry

+ Internal Security Strategy
+ European Agenda on Security

Environmental threats

DG ENV
Environment

Environment Action Programme
Directives: Seveso III, Water Framework, Floods

Climate threats

DG CLIMA
Climate action

EU Climate Adaptation Strategy

Health threats

DG SANTE
Consumer Health

Serious cross-border threats to health

International

DG DEVCO
International cooperation

CBRN-E Centres of Excellence

DG ENER
Energy

Trans-European Energy Instrastructure

DG MOVE
Transport

Tran-European Transport Network

DG TRADE

Transit of dual use items

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	SU-FCT01-2018-2019-2020: Human factors, and social, societal, and organizational aspects to solve issues in FCT **[sub-topic 2] - 2019 -** Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behavior **[sub-topic 4] - 2018 – 2019 –** Open	**2019**: 10.00	RIA - 100% €5M per project

Conditions –

- Active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries
- Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated
- Societal issues should be the core of the project (not technology)

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	**SU-FCT01-2018-2019-2020**: Human factors, and social, societal, and organizational aspects to solve issues in FCT **[sub-topic 2] - 2019 -** Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behavior **[sub-topic 4] - 2018 – 2019 –** Open	**2019**: 10.00	RIA - 100% €5M per project

Previously funded (open) –

- Investigate the influence of psychological and contextual human factors on the behavior of decision-making of police officers under stress and in high-risk operational situations
- Enhance societal CBRN preparedness by increasing practitioners' effectiveness in managing large, diverse groups of people in a CBRN environment

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	SU-FCT02-2018-2019-2020: Technologies to enhance FCT **[sub-topic 2] - 2019 –** Trace qualification - Forensic analysis of trace material **[sub-topic 4] - 2018 – 2019 - 2020 –** Open	**2019**: 28.16	RIA - 100% €7M per project

Conditions –

- TRL 4-6 (technology validated in lab - prototype demonstrated in relevant environment)
- Active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries
- Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	SU-FCT02-2018-2019-2020: Technologies to enhance FCT **[sub-topic 2] - 2019 –** Trace qualification - Forensic analysis of trace material **[sub-topic 4] - 2018 – 2019 - 2020 –** Open	**2019**: 28.16	RIA - 100% €7M per project

Previously funded (open) –

- Develop an advanced prediction, prevention, operation, and investigation platform by leveraging the IoT ecosystem, autonomous systems, and targeted technologies
- Achieving a significant increase in the speed of investigation processes and an improvement in identification of individuals

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism	**2019**: 8.00	IA - 70% €8M per project

Conditions –

- TRL 5-7 (technology validated-prototype demonstrated in relevant environment)
- Active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries
- Address trends in cybercrime and enhancing security of citizens in places considered soft targets
- Up to 24 months duration

Fight against Crime and Terrorism - FCT

Area	Topic	Budget (M€)	Funding Terms
Fight against Crime and Terrorism (FCT)	SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism	**2019**: 8.00	IA - 70% €8M per project

Previously funded –

- Establishing an open platform for providing cutting-edge practical support to LEAs in their fight against terrorism, organised crime and cybercrime. Increasing awareness regarding the state of the art and trends in cybercriminal activities to allow an in-depth knowledge of means of preventing and countering emerging and future cybercriminal activities

Policy Documents

- The European Agenda on Security
- ENISA, the "EU Cybersecurity Agency", Information and Communication Technology cybersecurity certification (''Cybersecurity Act“)
- Ninth progress report towards an effective and genuine Security Union
- Council Conclusions on the way forward in view of the creation of an European Forensic Science Area
- Eleventh progress report towards an effective and genuine Security Union

Border and External Security - BES

Area	Topic	Budget (M€)	Funding Terms
Border Security And External Security (BES)	SU-BES01-2018-2019-2020: Human factors, and social, societal, and organizational aspects of border and external security **[sub-topic 2] - 2019** - Modelling, predicting, and dealing with migration flows to avoid tensions and violence **[sub-topic 4] - 2018 – 2019 -** Open	**2019**: 10.00	RIA - 100% €5M per project

Conditions –

- ~~Active involvement of at least 3 Border or Coast Guards Authorities from at least 3 different EU or Associated countries~~
- ~~Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated~~
- Synergies and complementarity are pursued (e.g. KCMD, Societal Challenge 6)
- Border and Coast Guard Authorities are eligible. Their participation is encouraged

Border and External Security - BES

Area	Topic	Budget (M€)	Funding Terms
Border Security And External Security (BES)	SU-BES02-2018-2019-2020: Technologies to enhance border and external security **[sub-topic 3] - 2019 -** Security on-board passenger ships (full life cycle of the journey) **[sub-topic 4] - 2019 -** Detecting threats in the stream of commerce without disrupting business **[sub-topic 6] - 2018 – 2019 - 2020 –** Open	**2019**: 21.00	RIA - 100% €7M per project

Conditions –

- TRL 5-6 (technology validated-demonstrated in relevant environment)
- Active involvement of at least 3 Border or Coast Guards Authorities from at least 3 different EU or Associated countries
- Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated

Border and External Security - BES

Area	Topic	Budget (M€)	Funding Terms
Border Security And External Security (BES)	**SU-BES02-2018-2019-2020**: Technologies to enhance border and external security **[sub-topic 3] - 2019 -** Security on-board passenger ships (full life cycle of the journey) **[sub-topic 4] - 2019 -** Detecting threats in the stream of commerce without disrupting business **[sub-topic 6] - 2018 – 2019 - 2020 –** Open	**2019**: 21.00	RIA - 100% €7M per project

Previously funded (open) –

- Increase selective detection of trace levels of illicit drugs and their precursors. In the light of a strong need for better drug test systems at EU borders, this proposal addresses the development of a portable and wireless single prototype device with the capability to quickly test for different types of drugs, precursors , adulterants and cutting agents, with high accuracy

Border and External Security - BES

Area	Topic	Budget (M€)	Funding Terms
Border Security And External Security (BES)	**SU-BES03-2018-2019-2020**: Demonstration of applied solutions to enhance border and external security **[sub-topic 2] - 2019 -** New concepts for decision support and information systems **[sub-topic 4] - 2018 – 2019 - 2020 –** Open	**2019**: 10.00	IA - 70% €5M per project

Conditions –

- TRL 6-8 (technology demonstrated in relevant environment-system complete and qualified)
- Consortia must be coordinated by a practitioner organization (border/coast guard authority) under civilian authority and command
- Up to 18 months duration
- Demonstrate complementarity and no overlap with actions under PADR-US-01-2017

Border and External Security - BES

Area	Topic	Budget (M€)	Funding Terms
Border Security And External Security (BES)	**SU-BES03-2018-2019-2020:** Demonstration of applied solutions to enhance border and external security **[sub-topic 2] - 2019 -** New concepts for decision support and information systems **[sub-topic 4] - 2018 – 2019 - 2020 –** Open	**2019**: 10.00	IA - 70% €5M per project

Previously funded (open) –

- Develop and design advanced data fusion services and decision support services for the maritime surveillance domain

Policy Documents

Organised Crime & Human Trafficking

We help EU States in taking consistent action to effectively prevent and counter the many facets of modern organised crime.

+

THB Directive

Expl. of Children Directive

Serious and Organised Crime

Schengen, Borders & Visas

The EU's common external border calls for EU States' cooperation on border control and visa policy to ensure freedom and security within Europe.

+

Smart Borders

Interoperability of EU Information systems

European Border And Coast Guard

Document fraud

Irregular Migration & Return

In 2014, 276 113 migrants entered the EU irregularly via land, air and sea routes. Most migrants have recourse to criminal networks of smugglers.

+

EUROSUR

Migrant Smugg.

Taxation and Customs Union

EU Customs Strategy

Union Customs Code

Union External Security Policies in Civilian Tasks

CSDP

*COM(2018) 845 final - SU Progress Report, Dec. 2018 – State of play

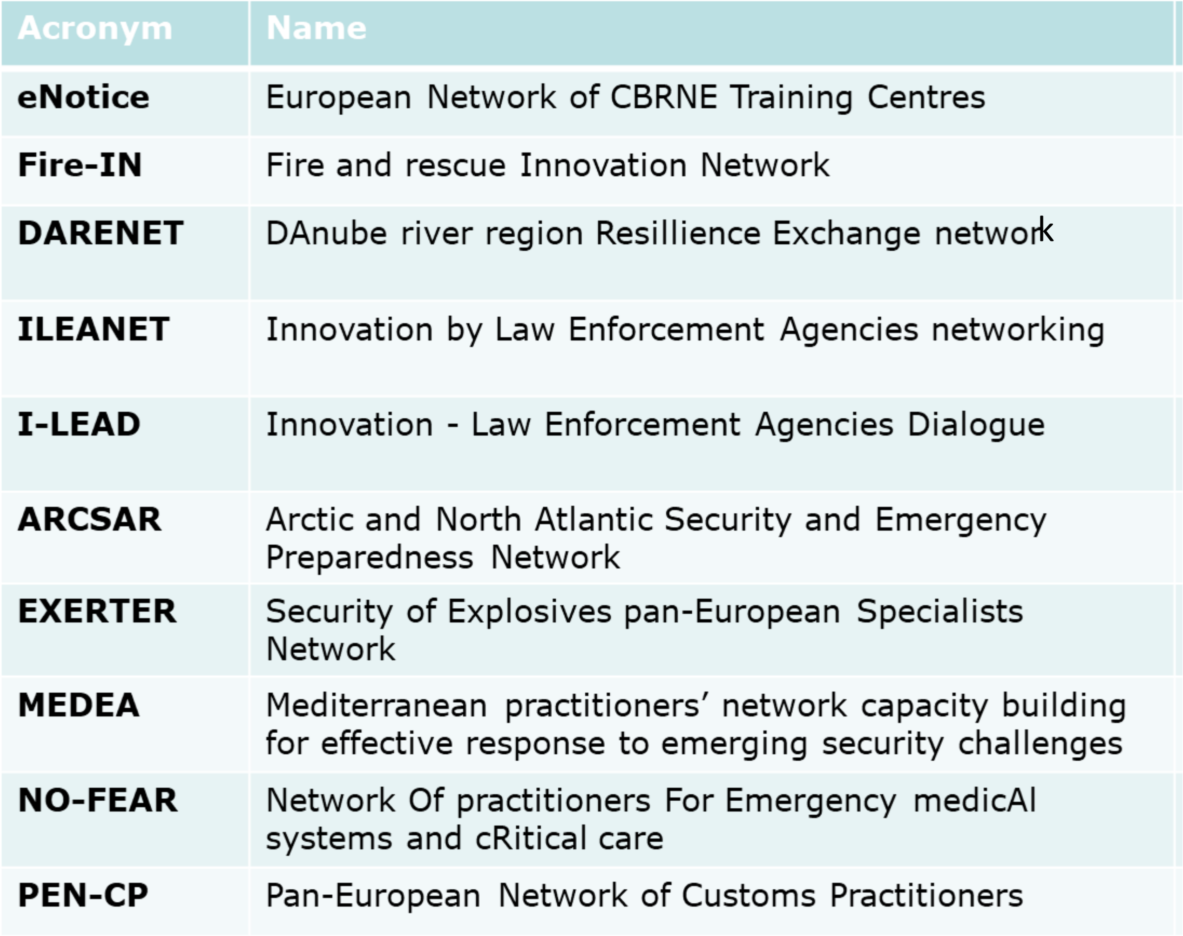
General Matters

Area	Topic	Budget (M€)	Funding Terms
General Matters	**SU-GM01-2018-2019-2020:** Pan-European networks of practitioners and other actors in the field of security **a. [2019-2020]** - Practitioners (end-users) in the same discipline and from across Europe – Hybrid Threats, ~~Protection of public figures~~	**2019:** 3.5	CSA - 100% €3.5M per project

Conditions –

- Practitioner participation from at least 8 Member States or Associated Countries is mandatory
- At least 25% of budget to interact with industry, academia, and other providers of innovative solutions outside of the consortium
- Each consortium must produce a report every 6 months (or less) about their findings
- Each proposal must include a workpackage to disseminate findings, including an annual workshop or conference
- One network chosen
- Recommended duration: 5 years

Practitioner Networks that Already Exist



Acronym	Name
eNotice	European Network of CBRNE Training Centres
Fire-IN	Fire and rescue Innovation Network
DARENET	DAnube river region Resillience Exchange network
ILEANET	Innovation by Law Enforcement Agencies networking
I-LEAD	Innovation - Law Enforcement Agencies Dialogue
ARCSAR	Arctic and North Atlantic Security and Emergency Preparedness Network
EXERTER	Security of Explosives pan-European Specialists Network
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges
NO-FEAR	Network Of practitioners For Emergency medicAl systems and cRitical care
PEN-CP	Pan-European Network of Customs Practitioners

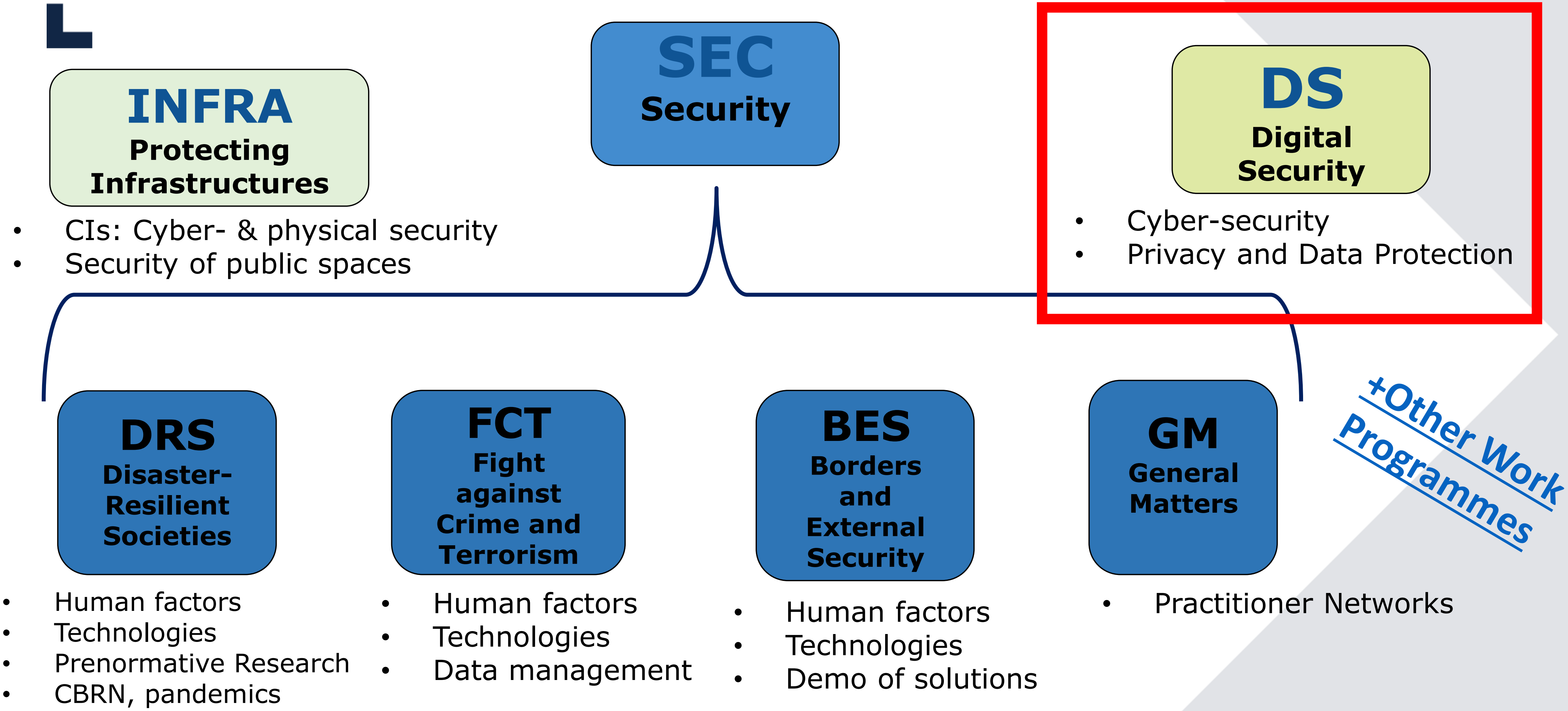
+ 2 new Networks (2018 call)

- Bring together infrastructure, equipment and experts from various organisations working in the field of radiological and nuclear (RN) emergencies
- Build a network of procurers in the security field

Policy Context

- Joint Framework on countering hybrid threats
- EC Press Release – 13.06.2018
- SEC Union Progress Report #15
- Increasing resilience and bolstering capabilities to address hybrid threats

Work Programme 2018-2020 - Structure



SEC
Security

INFRA
Protecting Infrastructures

- CIs: Cyber- & physical security
- Security of public spaces

DS
Digital Security

- Cyber-security
- Privacy and Data Protection

DRS
Disaster-Resilient Societies

- Human factors
- Technologies
- Prenormative Research
- CBRN, pandemics

FCT
Fight against Crime and Terrorism

- Human factors
- Technologies
- Data management

BES
Borders and External Security

- Human factors
- Technologies
- Demo of solutions

GM
General Matters

- Practitioner Networks

+Other Work Programmes

Cybersecurity

Area	Topic	Budget (M€)	Funding Terms
Cybersecurity, Digital Privacy and data protection	SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises **(a) [2019]:** Protecting citizens' security, privacy and personal data **(b) [2019]:** Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection	**2019**: 18.00	IA - 70% €4-5M per project

Conditions –

- Outcome TRL 7 (system prototype demonstrated in operational environment)
- End user involvement advised
- Synergies with data protection authorities and CERTs/CSIRTs recommended
- Specific attention to the gender dimension is required

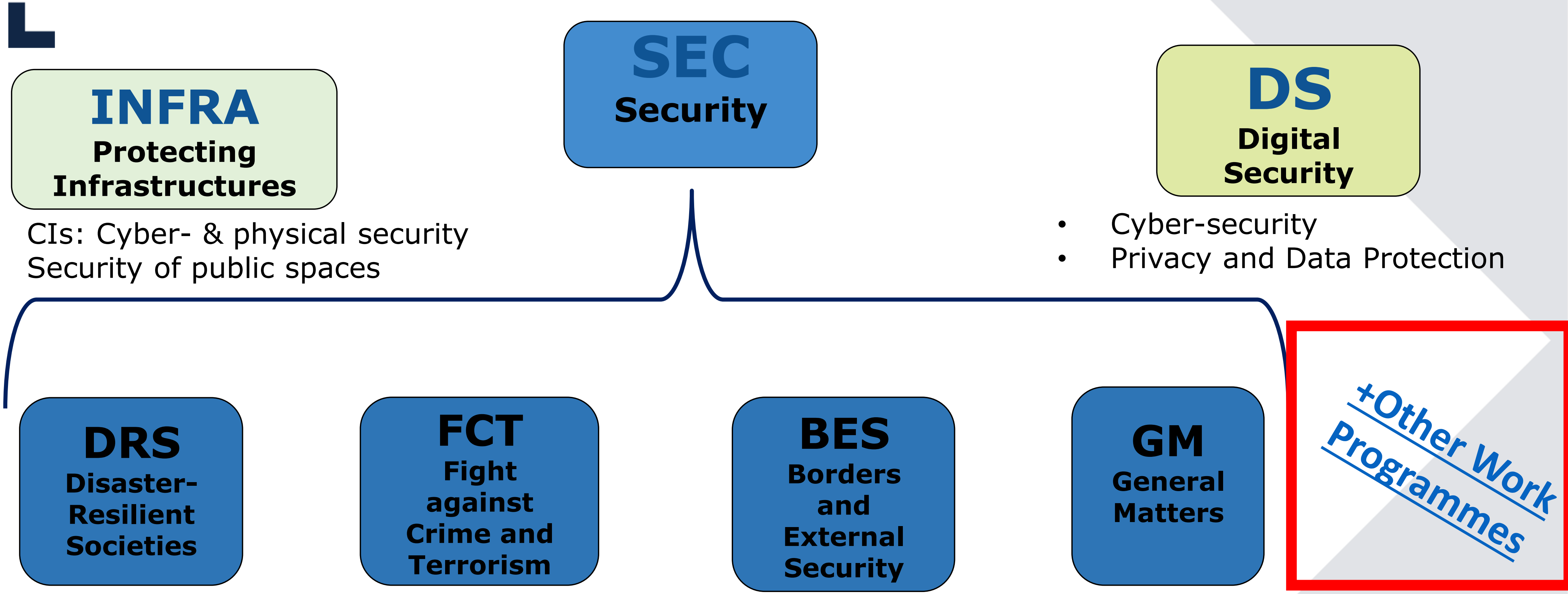
Cybersecurity

Area	Topic	Budget (M€)	Funding Terms
Cybersecurity, Digital Privacy and data protection	SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors **(a) [2019]:** Digital security, privacy and personal data protection in multimodal **transport** (IA) **(b) [2019]:** Digital security, privacy and personal data protection in **healthcare** ecosystem (RIA)	**2019**: 20.00 (10.00) each	IA - 70% €4M per project RIA – 100% €5M per project

Conditions –

- Outcome TRL 7 (system prototype demonstrated in operational environment)
- End user involvement advised
- Deliver specific social aspects of digital security related to training (practical, operational, hands-on training)
- Consider the relevant human factor and social aspects when developing innovative solutions.

Work Programme 2018-2020 - Structure



SEC
Security

INFRA
Protecting Infrastructures

- CIs: Cyber- & physical security
- Security of public spaces

DS
Digital Security

- Cyber-security
- Privacy and Data Protection

DRS
Disaster-Resilient Societies

- Human factors
- Technologies
- Prenormative Research
- CBRN, pandemics

FCT
Fight against Crime and Terrorism

- Human factors
- Technologies
- Data management

BES
Borders and External Security

- Human factors
- Technologies
- Demo of solutions

GM
General Matters

- Practitioner Networks

+Other Work Programmes

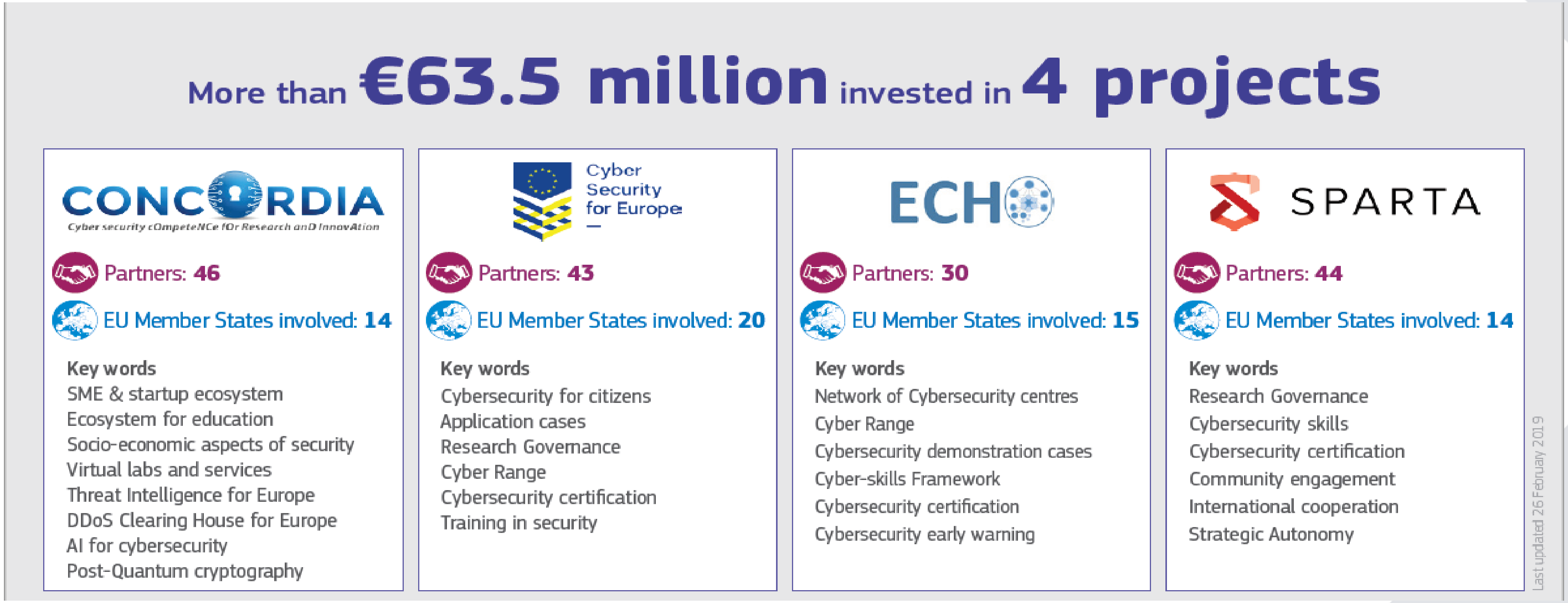
Other Related Topics

Area	Topic	Budget (M€)	Funding Terms
Information and Communication Technologies	SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (a) Cybersecurity/privacy audit, certification and standardization; (b) Trusted supply chains of ICT systems; (c) Designing and developing privacy-friendly and secure software and hardware;	47.00	RIA - 100% €4-5M per project

Conditions –

- Call deadline – 19.11.2019 (Open – 25.07.2019)
- Foresee actions to collaborate with projects funded under SU-ICT-03-2018
- Consider the relevant human factor and social aspects when developing innovative solutions
- Outcome TRL 5

Previously Funded Projects



More than **€63.5 million** invested in **4 projects**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**

EU Member States involved: **14**

Key words
SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography

Cyber Security for Europe

Partners: **43**

EU Member States involved: **20**

Key words
Cybersecurity for citizens
Application cases
Research Governance
Cyber Range
Cybersecurity certification
Training in security

ECHO

Partners: **30**

EU Member States involved: **15**

Key words
Network of Cybersecurity centres
Cyber Range
Cybersecurity demonstration cases
Cyber-skills Framework
Cybersecurity certification
Cybersecurity early warning

SPARTA

Partners: **44**

EU Member States involved: **14**

Key words
Research Governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic Autonomy

Last updated 26 February 2019

Cascade Funding

Cascade Funding, also known as Financial Support for Third Parties (FSTP), is a European Commission mechanism to simplify the administrative procedures by allowing some EU-funded projects to issue open calls for further funding

BroadWay Project –

Call for a Broadband mobile system for Public Protection and Disaster Relief (PPDR).

Deadline – 03.06.2019

Phase 1 – Planning the solution (max 73,687.99 euro) – 6 months

Phase 2 – For those who pass Phase 1 - Prototype (max 1,407,921.73 euro) – up to a year

Phase 3 – Foe those who pass Phase 2 - Pilot (max 1,502,247.43 euro) – up to 11 months

SHUTTLE Project –

Call for a toolkit for forensic identification.

Phase 1 – Solution design – 3-6 months – 4 suppliers (1,200,000 euro)

Phase 2 – For those who pass Phase 1 - Prototype – 6-12 months – 3 suppliers (3,000,000 euro)

Phase 3 – For those who pass Phase 2 - Testing – 6-12 months – 2 suppliers (3,200,000 euro)

Become an Expert Evaluator

The benefits of being an evaluator:

- Learning the process and evaluating
- Meeting evaluators from across Europe and themes
- Learning the current thinking and state of the art
- Become part of the community
- Facilitate your own future participation in the program!

Industrial background / Female candidate
might give an advantage

Red Team

"A red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view."

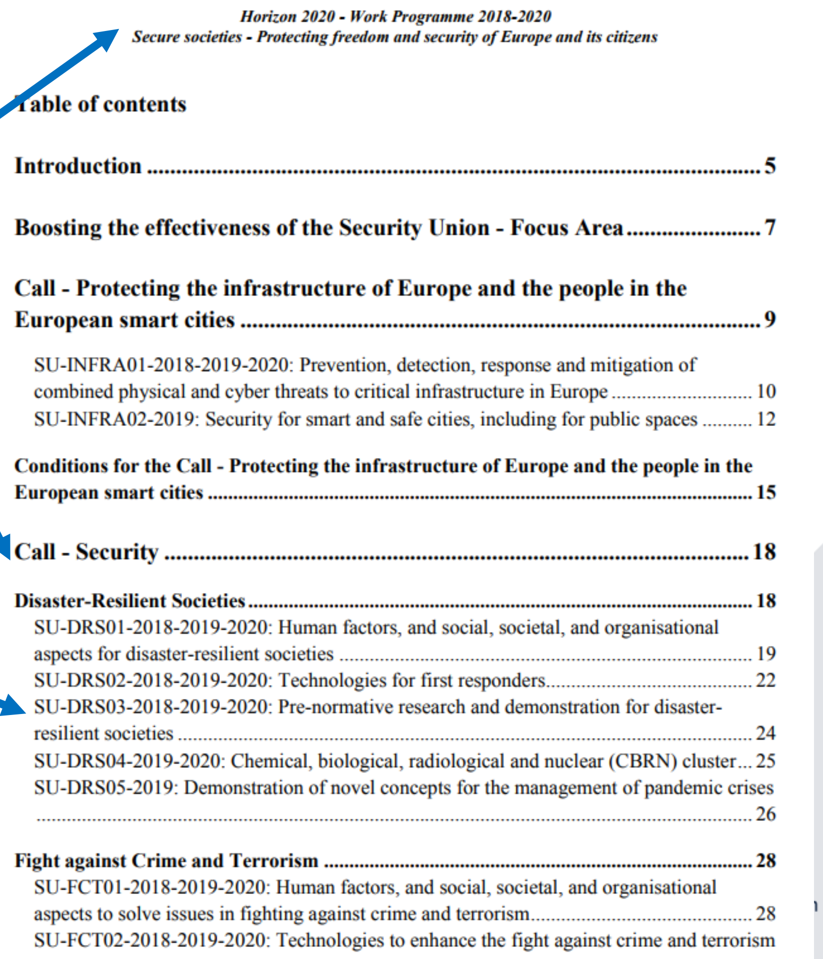
- Wikipedia

The Red Team service is a national full proposal check -

- It is free of charge
- It uses expert reviewers of the Innovation Authority, many of which are also H2020 reviewers
- All reviewers have signed NDA with the Innovation Authority
- The identity of the reviewer is classified
- The full proposal must be submitted **at least a month in advance** of the topic deadline

Reading the Work Programme

- Get familiar with the [Funding and Tenders Portal]
- Read the Work Programme/s (WP) carefully
- Identify the subject/s of your expertise/interest in the WP
- Verify that the relevant call is open
- Check for “best fit” topic/s

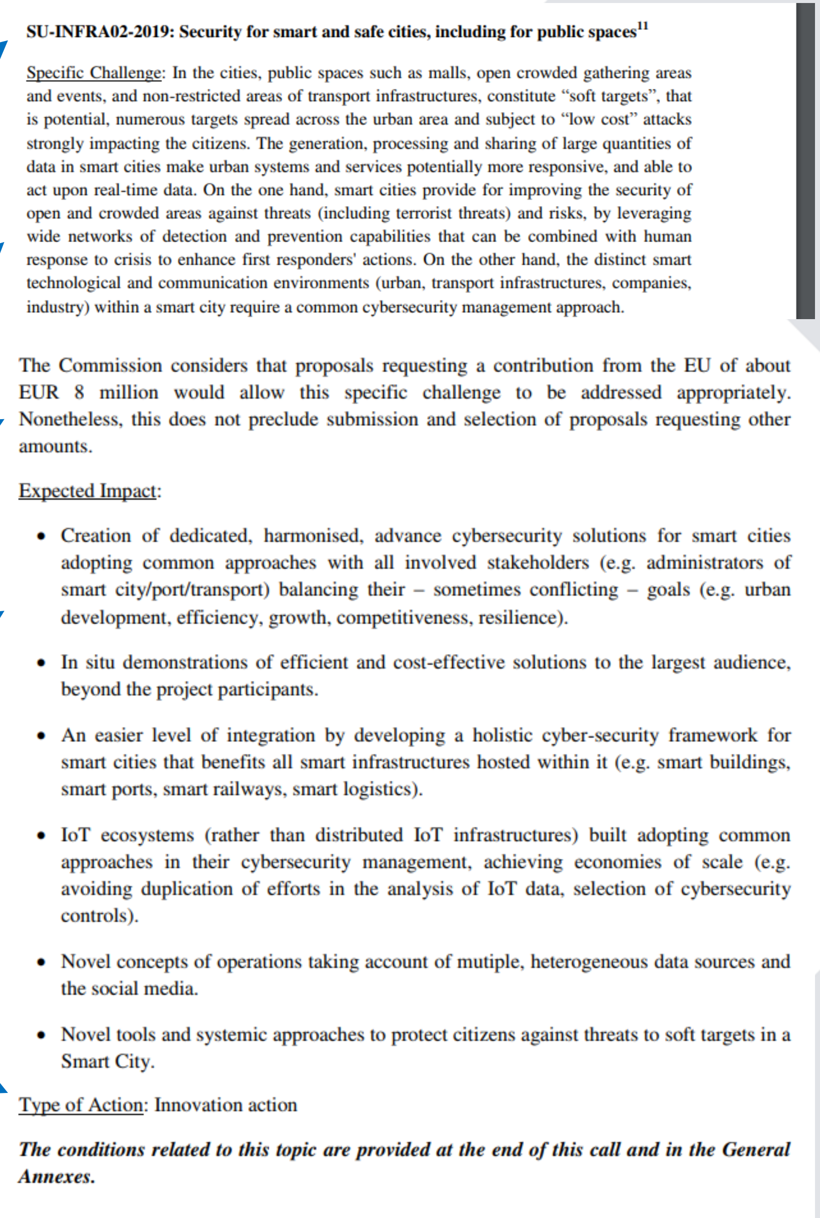


Horizon 2020 - Work Programme 2018-2020
Secure societies - Protecting freedom and security of Europe and its citizens

Table of contents

Know Your Topic

- Topic name
- The challenge a solution is needed for
- Expected budget
- Expected impact of your project
- Type of action



SU-INFRA02-2019: Security for smart and safe cities, including for public spaces[11]

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.

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:

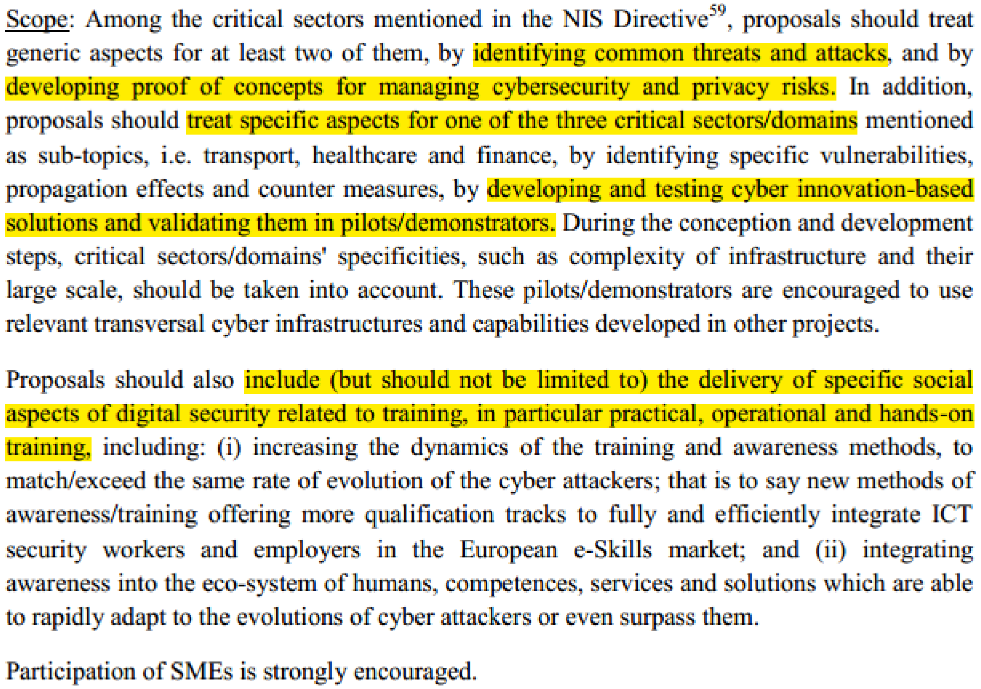
- Creation of dedicated, harmonised, advance cybersecurity solutions for smart cities adopting common approaches with all involved stakeholders (e.g. administrators of smart city/port/transport) balancing their – sometimes conflicting – goals (e.g. urban development, efficiency, growth, competitiveness,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

Type of Action: Innovation action

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

Proposal Sections

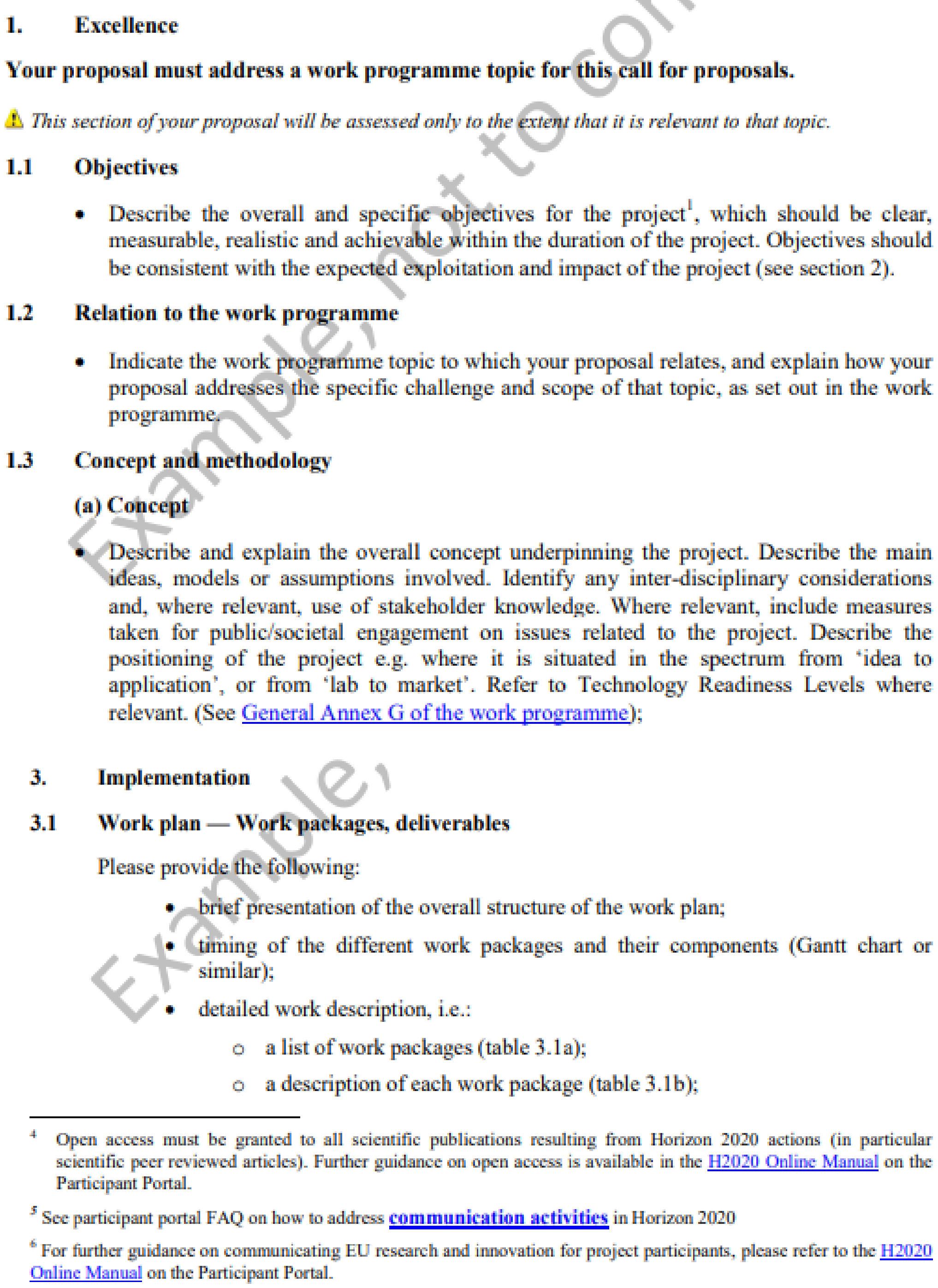
- The Call text sections correspond with the proposal sections
  - ○ Scope = Excellence (section B1) and Implementation (section B3)



Scope: Among the critical sectors mentioned in the NIS Directive[59], 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.



1. Excellence

Your proposal must address a work programme topic for this call for proposals.

⚠ *This section of your proposal will be assessed only to the extent that it is relevant to that topic.*

1.1 Objectives

- Describe the overall and specific objectives for the project[4], which should be clear, measurable, realistic and achievable within the duration of the project. Objectives should be consistent with the expected exploitation and impact of the project (see section 2).

1.2 Relation to the work programme

- Indicate the work programme topic to which your proposal relates, and explain how your proposal addresses the specific challenge and scope of that topic, as set out in the work programme.

1.3 Concept and methodology

(a) Concept

- Describe and explain the overall concept underpinning the project. Describe the main ideas, models or assumptions involved. Identify any inter-disciplinary considerations and, where relevant, use of stakeholder knowledge. Where relevant, include measures taken for public/societal engagement on issues related to the project. Describe the positioning of the project e.g. where it is situated in the spectrum from 'idea to application', or from 'lab to market'. Refer to Technology Readiness Levels where relevant. (See General Annex G of the work programme);

3. Implementation

3.1 Work plan — Work packages, deliverables

Please provide the following:

- brief presentation of the overall structure of the work plan;
- timing of the different work packages and their components (Gantt chart or similar);
- detailed work description, i.e.:
  - ○ a list of work packages (table 3.1a);
  - ○ a description of each work package (table 3.1b);

[4] Open access must be granted to all scientific publications resulting from Horizon 2020 actions (in particular scientific peer reviewed articles). Further guidance on open access is available in the H2020 Online Manual on the Participant Portal.

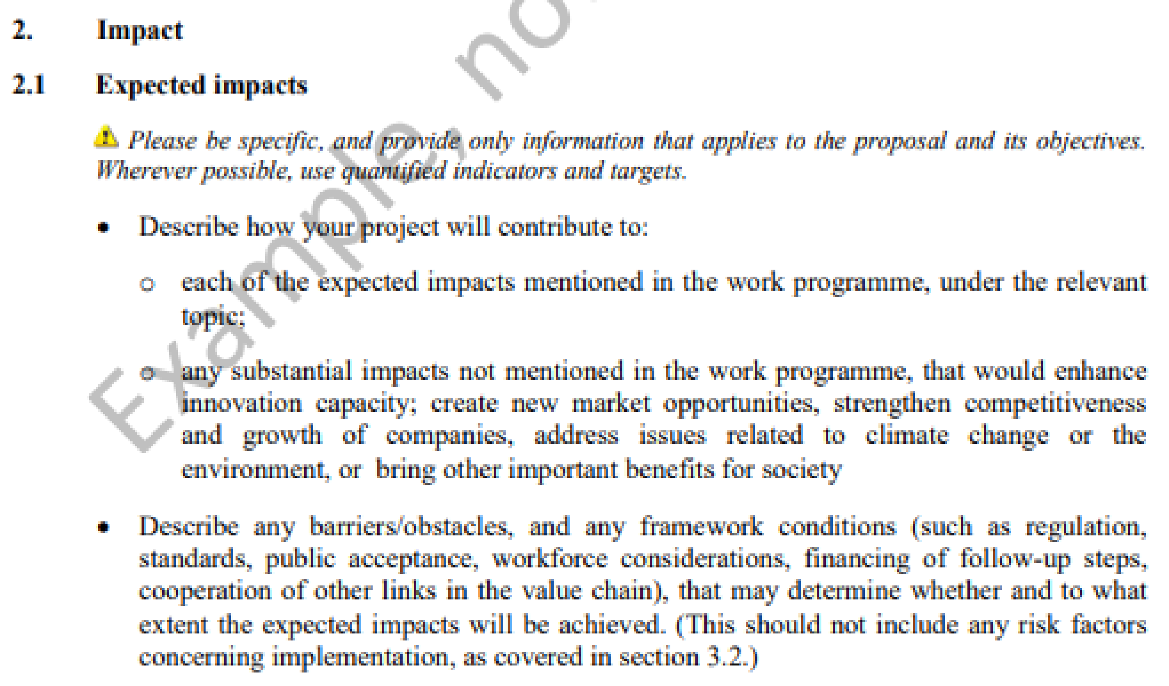
[5] See participant portal FAQ on how to address **communication activities** in Horizon 2020

[6] For further guidance on communicating EU research and innovation for project participants, please refer to the H2020 Online Manual on the Participant Portal.

Proposal Sections

- The Call text sections correspond with the [proposal sections]

  - ○ Impact = Impact (section B2)
  - ○ **All** impacts listed in the call text must be addressed

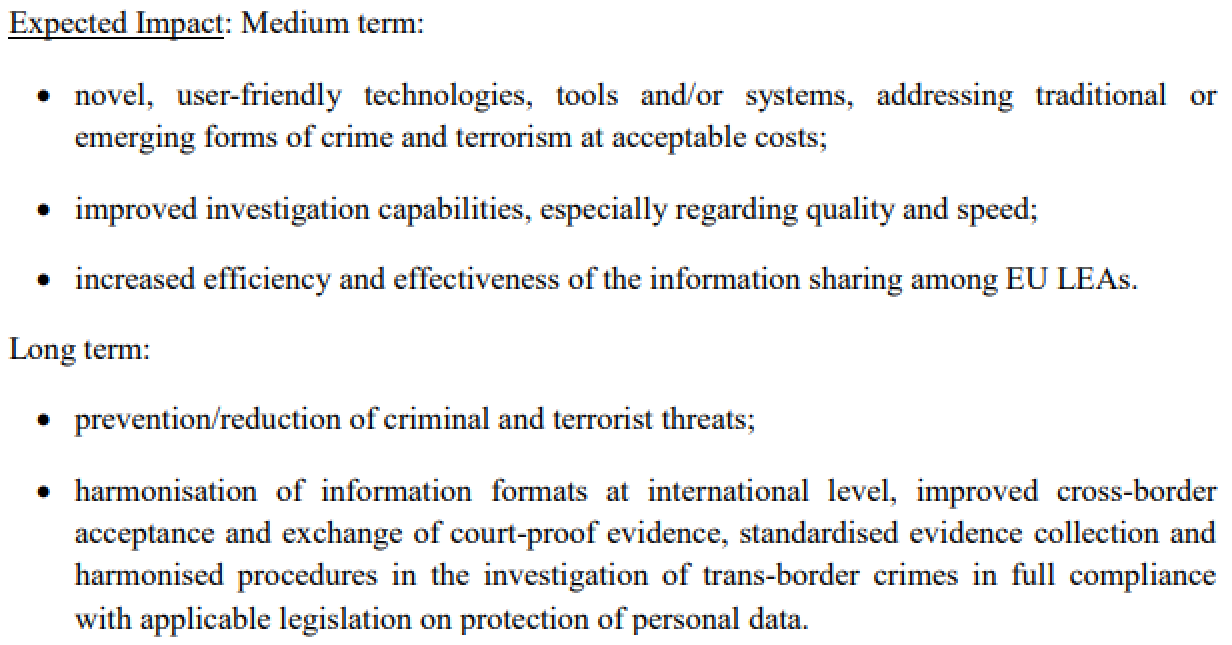


2. **Impact**

2.1 **Expected impacts**

⚠ *Please be specific, and provide only information that applies to the proposal and its objectives. Wherever possible, use quantified indicators and targets.*

- Describe how your project will contribute to:
  - ○ each of the expected impacts mentioned in the work programme, under the relevant topic;
  - ○ any substantial impacts not mentioned in the work programme, that would enhance innovation capacity; create new market opportunities, strengthen competitiveness and growth of companies, address issues related to climate change or the environment, or bring other important benefits for society
- Describe any barriers/obstacles, and any framework conditions (such as regulation, standards, public acceptance, workforce considerations, financing of follow-up steps, cooperation of other links in the value chain), that may determine whether and to what extent the expected impacts will be achieved. (This should not include any risk factors concerning implementation, as covered in section 3.2.)



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.

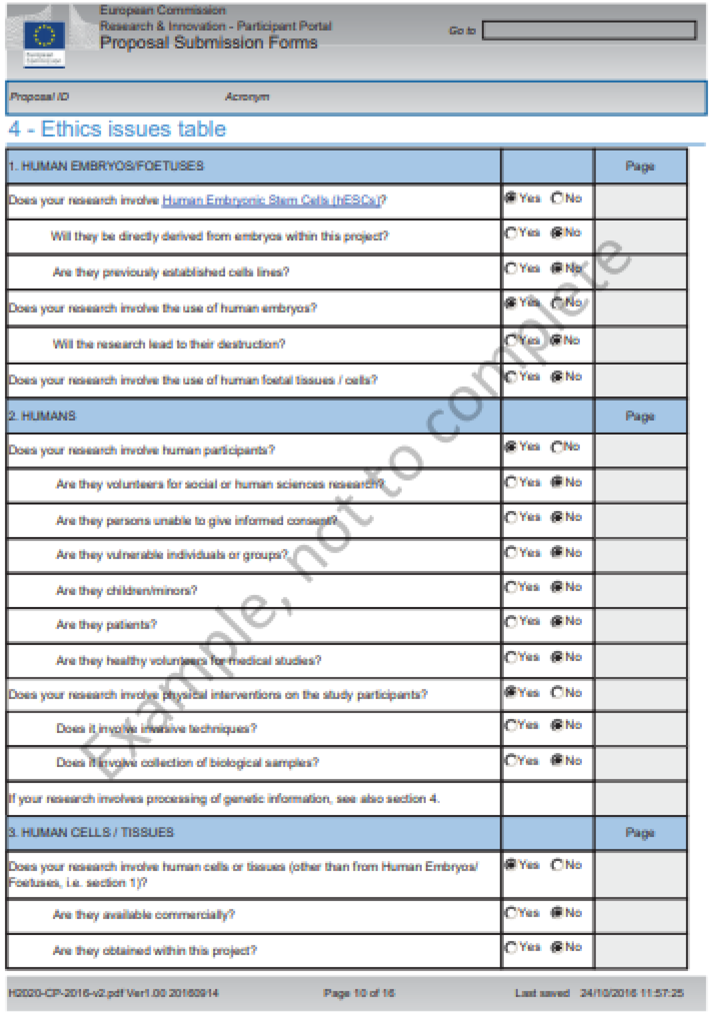
Long term:

- 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.

Proposal Sections

Take note of any Ethics requirements - the ethics table always needs to be filled in, even if you are just writing that there are no issues

Additional Ethics information



European Commission
Research & Innovation - Participant Portal
Proposal Submission Forms

Go to

Proposal ID   Acronym

4 - Ethics issues table

1. HUMAN EMBRYOS/FOETUSES		Page
Does your research involve Human Embryonic Stem Cells (hESCs)?	● Yes ○ No	
Will they be directly derived from embryos within this project?	○ Yes ● No	
Are they previously established cells lines?	○ Yes ● No	
Does your research involve the use of human embryos?	● Yes ○ No	
Will the research lead to their destruction?	○ Yes ● No	
Does your research involve the use of human foetal tissues / cells?	○ Yes ● No	
2. HUMANS		Page
Does your research involve human participants?	● Yes ○ No	
Are they volunteers for social or human sciences research?	○ Yes ● No	
Are they persons unable to give informed consent?	○ Yes ● No	
Are they vulnerable individuals or groups?	○ Yes ● No	
Are they children/minors?	○ Yes ● No	
Are they patients?	○ Yes ● No	
Are they healthy volunteers for medical studies?	○ Yes ● No	
Does your research involve physical interventions on the study participants?	● Yes ○ No	
Does it involve invasive techniques?	○ Yes ● No	
Does it involve collection of biological samples?	○ Yes ● No	
If your research involves processing of genetic information, see also section 4.		
3. HUMAN CELLS / TISSUES		Page
Does your research involve human cells or tissues (other than from Human Embryos/ Foetuses, i.e. section 1)?	● Yes ○ No	
Are they available commercially?	○ Yes ● No	
Are they obtained within this project?	○ Yes ● No	

H2020-CP-2016-v2.pdf Ver1.00 20160914   Page 10 of 16   Last saved 24/10/2016 11:57:25

European Commission

The EU Framework Programme for Research and Innovation

HORIZON 2020

H2020 Programme

Proposal template 2018-2020

Administrative forms (Part A)
Project proposal (Part B)

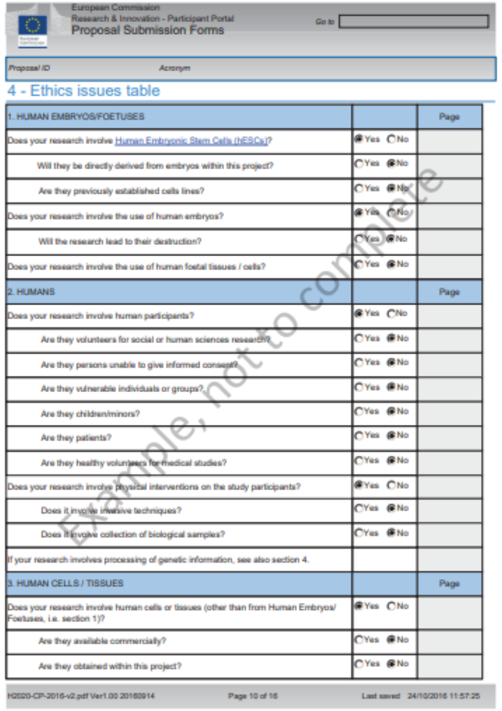
Research and Innovation Actions (RIA)
Innovation Actions (IA)

Version 3.4
1 February 2018

Disclaimer
This document is aimed at informing potential applicants for Horizon 2020 funding. It serves only as an example. The actual Web forms and templates, provided in the online proposal submission system under the Participant Portal, might differ from this example. Proposals must be prepared and submitted via the online proposal submission system under the Participant Portal.

Ethics Review

- For main and reserve list proposals **an ethics screening** and, if required, an ethics assessment is carried out **by independent ethics experts** *after* the scientific evaluation
- The **experts will assess whether the ethics issues are adequately addressed**
- The ethics experts will produce an ethics report and give an opinion on the proposal, such as:
  - Granting ethics clearance (or not)
  - Recommending the inclusion of 'ethics requirements' in the grant agreement
  - Recommending a further Ethics Assessment and/or an Ethics Check or Audit



European Commission
Research & Innovation - Participant Portal
Proposal Submission Forms

Proposal ID Acronym

4 - Ethics issues table

1. HUMAN EMBRYOS/FOETUSES		Page
Does your research involve Human Embryonic Stem Cells (hESCs)?	● Yes ○ No	
Will they be directly derived from embryos within this project?	○ Yes ● No	
Are they previously established cells lines?	○ Yes ● No	
Does your research involve the use of human embryos?	● Yes ○ No	
Will the research lead to their destruction?	○ Yes ● No	
Does your research involve the use of human foetal tissues / cells?	○ Yes ● No	
2. HUMANS		**Page**
Does your research involve human participants?	● Yes ○ No	
Are they volunteers for social or human sciences research?	○ Yes ● No	
Are they persons unable to give informed consent?	○ Yes ● No	
Are they vulnerable individuals or groups?	○ Yes ● No	
Are they children/minors?	○ Yes ● No	
Are they patients?	○ Yes ● No	
Are they healthy volunteers for medical studies?	○ Yes ● No	
Does your research involve physical interventions on the study participants?	● Yes ○ No	
Does it involve invasive techniques?	○ Yes ● No	
Does it involve collection of biological samples?	○ Yes ● No	
If your research involves processing of genetic information, see also section 4.		
3. HUMAN CELLS / TISSUES		**Page**
Does your research involve human cells or tissues (other than from Human Embryos/ Foetuses, i.e. section 1)?	● Yes ○ No	
Are they available commercially?	○ Yes ● No	
Are they obtained within this project?	○ Yes ● No	

H2020-CP-2016-v2.pdf Ver1.00 20160914 Page 10 of 16 Last saved 24/10/2016 11:57:25

ISERD
המנהלת הישראלית למו"פ האירופי
Israel-Europe R&I Directorate

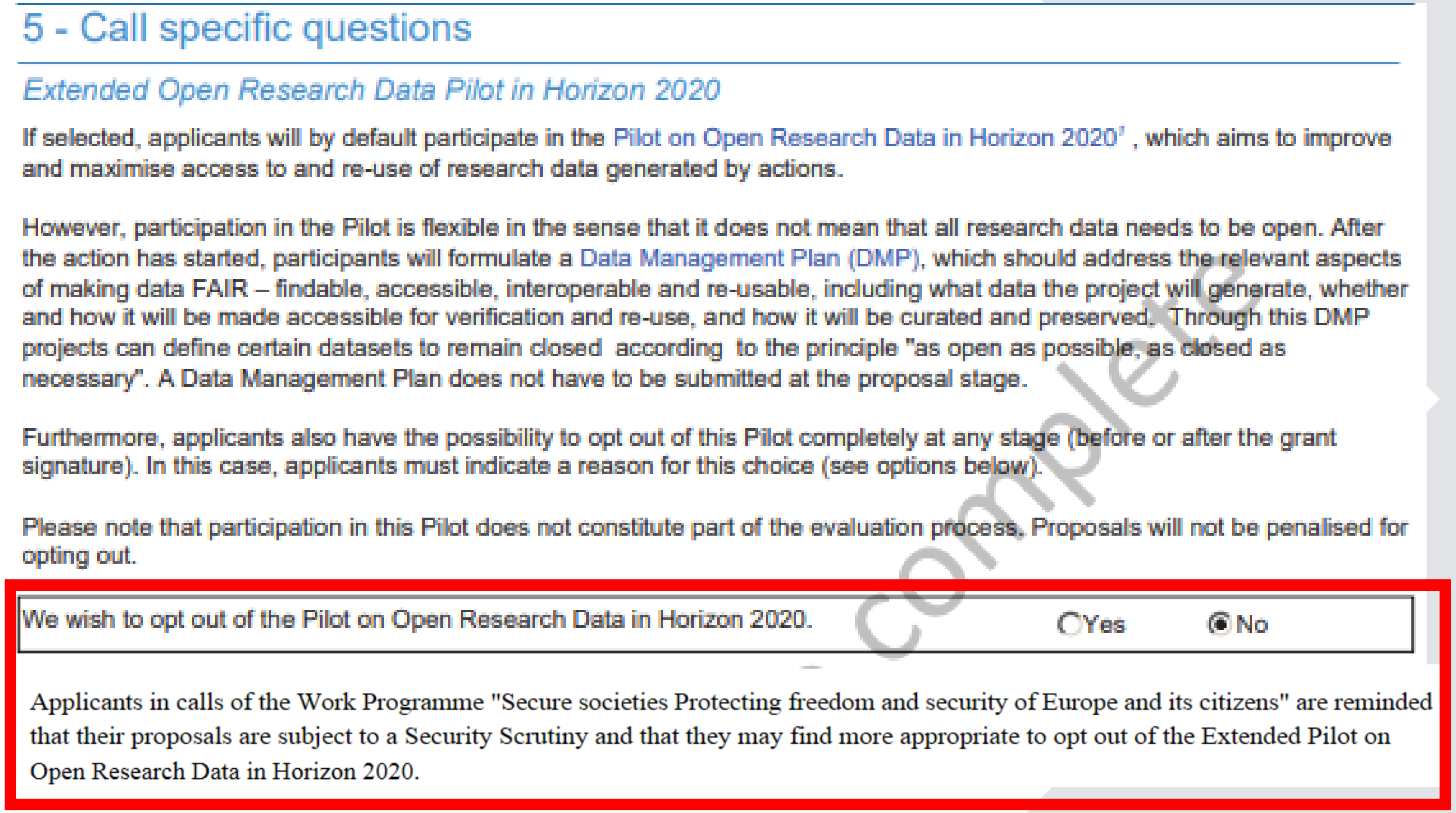
רשות החדשנות
Israel Innovation Authority

Ministry of Science Technology & Space

המועצה להשכלה גבוהה
COUNCIL FOR HIGHER EDUCATION
הוועדה לתכנון ולתקצוב
PLANNING & BUDGETING COMMITTEE

Open Access to Data

- You can opt out of the Open Research Data Pilot (you still need to pass a security scrutiny)
- This does not affect the score you get in any way
- Choice can be changed at any time before or after GA signature



5 - Call specific questions

Extended Open Research Data Pilot in Horizon 2020

If selected, applicants will by default participate in the Pilot on Open Research Data in Horizon 2020[1] , which aims to improve and maximise access to and re-use of research data generated by actions.

However, participation in the Pilot is flexible in the sense that it does not mean that all research data needs to be open. After the action has started, participants will formulate a Data Management Plan (DMP), which should address the relevant aspects of making data FAIR – findable, accessible, interoperable and re-usable, including what data the project will generate, whether and how it will be made accessible for verification and re-use, and how it will be curated and preserved. Through this DMP projects can define certain datasets to remain closed according to the principle "as open as possible, as closed as necessary". A Data Management Plan does not have to be submitted at the proposal stage.

Furthermore, applicants also have the possibility to opt out of this Pilot completely at any stage (before or after the grant signature). In this case, applicants must indicate a reason for this choice (see options below).

Please note that participation in this Pilot does not constitute part of the evaluation process. Proposals will not be penalised for opting out.

We wish to opt out of the Pilot on Open Research Data in Horizon 2020.	○ Yes	● No

Applicants in calls of the Work Programme "Secure societies Protecting freedom and security of Europe and its citizens" are reminded that their proposals are subject to a Security Scrutiny and that they may find more appropriate to opt out of the Extended Pilot on Open Research Data in Horizon 2020.

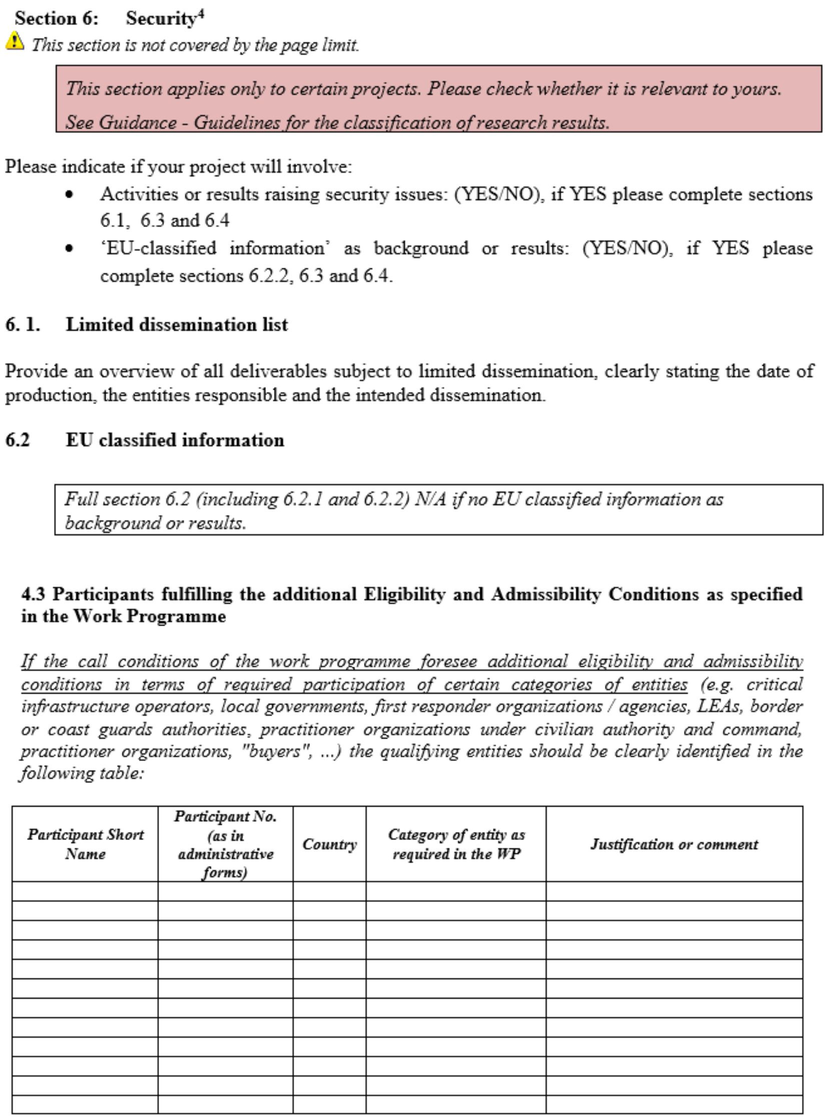
Security Scrutiny Procedure

- The Security Scrutiny Group is made up of one expert from each MS or AC represented in the proposal - they verify that all security aspects are properly addressed
- The scrutiny procedure is done in a 2 month period, following the technical evaluation and before the start of the GAP (Grant Agreement Procedure)
- The results of the scrutiny could be:
  - Go ahead with GAP;
  - Recommendations for the GAP without classification;
  - Recommendations for the GAP with classification (EU SECRET, EU CONFIDENTIAL, EU RESTRICTED);
  - Recommendation not to finance the proposal
- Applicants receive the conclusions of the scrutiny procedure with the “Information letter” via the Participant Portal

Admissibility Conditions

- Page limits – sections 1-3 - Limit: 70 pages (RIA/IA/PCP), 50 (CSA); all excess pages appear blank – do not play games!!! (no restriction on sections 4-6)
- Section 6 (Security) is unique to all SEC, INFRA and DS proposals
- Section 4.3 (practitioner self-declaration table) is unique to all SEC and INFRA proposals
- Minimum font allowed – 11
- Margins – at least 15mm (without footers or headers)
- Be clear in the proposal – who is the practitioner/end

user required – do not make the evaluator guess



Section 6: Security[4]

⚠ *This section is not covered by the page limit.*

This section applies only to certain projects. Please check whether it is relevant to yours.
See Guidance - Guidelines for the classification of research results.

Please indicate if your project will involve:

- Activities or results raising security issues: (YES/NO), if YES please complete sections 6.1, 6.3 and 6.4
- 'EU-classified information' as background or results: (YES/NO), if YES please complete sections 6.2.2, 6.3 and 6.4.

6. 1. Limited dissemination list

Provide an overview of all deliverables subject to limited dissemination, clearly stating the date of production, the entities responsible and the intended dissemination.

6.2 EU classified information

Full section 6.2 (including 6.2.1 and 6.2.2) N/A if no EU classified information as background or results.

4.3 Participants fulfilling the additional Eligibility and Admissibility Conditions as specified in the Work Programme

If the call conditions of the work programme foresee additional eligibility and admissibility conditions in terms of required participation of certain categories of entities (e.g. critical infrastructure operators, local governments, first responder organizations / agencies, LEAs, border or coast guards authorities, practitioner organizations under civilian authority and command, practitioner organizations, "buyers", ...) the qualifying entities should be clearly identified in the following table:

Participant Short Name	*Participant No. (as in administrative forms)*	*Country*	*Category of entity as required in the WP*	*Justification or comment*

General Tips

- English, English, English – make sure your points come across in clear English that can be understood and is structured properly – an annoyed reviewer is not a happy one!
- Be aware of, and reference, policy documents – The reviewers and Commission want to see you know what their goals are and your project is aligned with them

General Tips

- If you have many acronyms, add a page with a list of all of them at the end
- Use pictures, diagrams or charts to convey your point – these should be large enough to read, and high quality, don’t include reduced pictures of tables and text to save space
- Download your proposal to see that all the charts and pictures look OK

General Tips

- Letters of intent are important – it shows you are serious and that you have stakeholders engaged
- Make sure you **<u>follow the rules </u>**– involve enough practitioners as beneficiaries with significant jobs – do not get disqualified on a technicality (and do not make the reviewer guess who the practitioners are – fill in table 4.3)

General Tips

- Write actual risks and a mitigation plan to show you have thought the idea through
- Gender reference does not mean making sure there are 50% men and women in the consortia, but rather should be addressed as a research parameter

General Tips

- Benefits of the proposal are an important issue – for the society, for the economy, for climate change, etc. Address these benefits clearly - they are a selling point
- Explain the value of your proposal – how is your solution beyond the state of the art, what are your key resources, customer relationship, distribution channels, customer segments, etc.

General Tips

- If you are resubmitting a proposal, go over the state of the art and update this section since it has probably changed. Check the requirements of the topic as well since they may be updated (LEA involvement for example)
- A mini business model needs to be created in the proposal – make sure you answer - who your strategic partners are, and what your key activities are

General Tips

- A mini elevator pitch can be put in the excellence section to convince the evaluators you are solving the problem presented
    - Template – For (the target customer), who has (the customer needs), (the product name) is a (market category) that (main key benefit). Unlike (the competition) the product we have (unique difference).
        - Example - For first responders who have a need to locate as many live victims as possible, FINDLIFE is a platform that combines data from many different sources in order to find more live victims. Unlike the solutions currently available, our product is based on simultaneous use of sensors and human generated data, providing AI powered guidance to rescue teams.

General Tips

- Brexit – UK entities are considered according to their current status – Member States. However, if there is no agreement with the EU, there will be no funding for UK entities in projects already approved (there may be funding from the UK government). If they choose to leave the project due to lack of funding, the project still needs to meet the Call criteria. If there is a UK LEA, make sure there is one extra in case they leave, so that you still meet the minimum.

General Tips

- Don’t put too many PM in one WP – it shows an uneven distribution of work
- Read previous winning project ideas to see what has already been funded and what gaps still exist – do not duplicate existing project ideas or solutions – they will not be funded
- Consult FAQ for more information

General Tips

- Resubmitting a proposal under an open sub topic (that was previously submitted to a different sub topic) is possible, but eligibility conditions need to change
- Sources – add hyperlinks or link addresses in footnotes
- Many times proposers focus more on the technology, and not on the solution – both are important

General Tips

- Do not wait until the final day of the deadline to submit your proposal. It is better to upload a version in advance, any version uploaded after this will replace previous versions in the system
- Supporting Docs for operational capacity assessment:
  - CVs of responsible / key persons
  - ~5 relevant publications / products / services
  - Description of infrastructure / equipment (if relevant)
  - Possible 3rd party involvement

ISERD

המינהלת הישראלית למו״פ האירופי

Israel-Europe R&I Directorate

THANK YOU

INNOVATION

BREAKS BOUNDARIES

www.iserd.org.il

רשות החדשנות
Israel Innovation
Authority

Ministry of Science
Technology & Space

המועצה
להשכלה
גבוהה

مجلس
التعليم
العالي

COUNCIL FOR HIGHER EDUCATION
הועדה לתכנון ולתקצוב
PLANING & BUDGETING COMMITTEE