







THE EU RESEARCH & INNOVATION PROGRAMME

2021 – 2027

Cluster 3: Civil Security for Society

SSRI Destination

Research and Innovation David RIOS MORENTIN
European Commission - DG HOME
Innovation and Security Research Unit

Destination "Strengthened Security Research and Innovation"

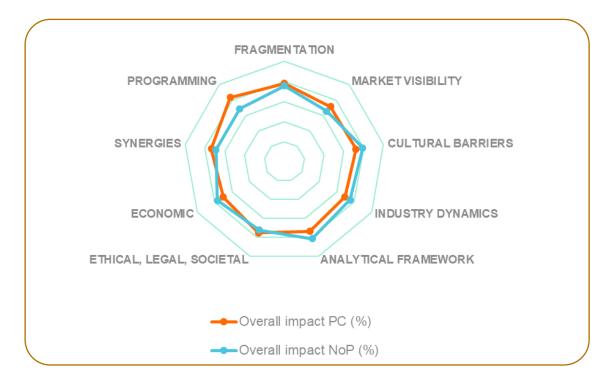
CALL 2021





Strengthened Security R&I (SSRI)

- EU investment for the development of capabilities supporting policy priorities
 - Innovation can be decisive: modernisation / effectiveness / efficiency
 - Uptake of innovation remains a challenge



- Create a favourable environment to generate specific knowledge
- Foster a structured dialogue and coordinated action among market actors;

European

- Exploit catalysts of uptake
- Conduct cross-cutting security research.

SSRI Destination

Stronger pillars of security Research and Innovation

 A more effective and efficient evidence-based development of EU civil security capabilities built on a stronger, more systematic and analysis-intensive security R&I cycle

Increased Innovation uptake of security R&I outcomes

 Increased industrialisation, commercialisation, adoption and deployment of successful outcomes of security research reinforces the competitiveness and resilience of EU security technology and industrial base

Cross-cutting knowledge for common security solutions

• R&I-enabled knowledge and value in cross-cutting matters reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions



Uptake Factors Vs. Topics 2021-2022

Sub area	Topic Ref.	Topic title	Fragmentation	Market Visibility	Cultural Barriers	Industry Dynamics	Analytical Framework	ELSE	Synergies	Programming
1	2021-SSRI-01-01	A maturity assessment framework for security technologies	*	*			*			*
1	2022-SSRI-01-01	Increased foresight capacity for security			*		*	*		*
1	2021-SSRI-01-02	Knowledge Networks for Security Research & Innovation - BM, INFRA	*	*			*			*
1	2022-SSRI-01-02	Knowledge Networks for security Research & Innovation - DRS, FCT	*	*			*			*
1	2021-SSRI-01-03	National Contact Points (NCPs) in the field of security and cybersecurity	*	*					*	*
2	2021-SSRI-01-04	Demand-led innovation for situation awareness in civil protection		*	*	*			*	
2	2022-SSRI-01-03	Stronger grounds for pre-commercial procurement of innovative security technologies		*	*	*			*	
3	2021-SSRI-01-05	Societal Impact assessment and impact creation			*		*	*		
3	2022-SSRI-01-04	Social innovations as enablers of security solutions and increased security perception			*		*	*		



SSRI Destination budget



Call	Budgets (EUR millio	Deadline(s)	
	2021	2022	
HORIZON-CL3-2021-SSRI-01	16.00		23 Nov 2021
HORIZON-CL3-2022-SSRI-01		9.50	23 Nov 2022
Overall indicative budget	16.00	9.50	

Topics	Type of Budgets (EUR Action million)		Expected EU contribution per	Number of projects		
		2021	project (EUR million)	expected to be funded		
Opening: 30 Jun 2021						
	Deadline(s): 23 Nov 2021				
HORIZON-CL3-2021-SSRI-01-01	RIA	1.50	Around 1.50	1		
HORIZON-CL3-2021-SSRI-01-02	CSA	4.00	Around 2.00	2		
HORIZON-CL3-2021-SSRI-01-03	CSA	2.50	Around 2.50	1		
HORIZON-CL3-2021-SSRI-01-04	PCP	6.00	Around 6.00	1		
HORIZON-CL3-2021-SSRI-01-05	RIA	2.00	Around 2.00	1		
Overall indicative budget		16.00				



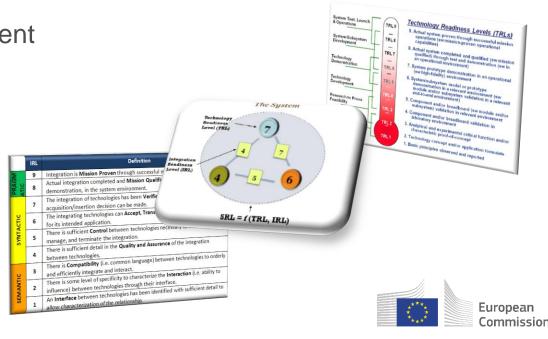
2021-SSRI-01-01: A maturity assessment framework for security technologies

Topics	Type of Action	Budgets (EUR million) 2021		Number of projects expected to be funded
			project (EOK IIIIIIOII)	
HORIZON-CL3-2021-SSRI-01-01	RIA	1.50	Around 1.50	1

- Expected outcome
 - Increased literacy on the value and efficient use of maturity assessment frameworks in security;
 - Common harmonised analytical frameworks for the security domain;
 - Widely accessible assessment tools and methods;
 - Evidence-based programming of security research built on a more reliable assessment of the state
 of the art of security tec.

2021-SSRI-01-01: A maturity assessment framework for security technologies

- Measure the progress of the development of innovative technologies to support decision making for further investment and uptake;
- Readiness, not only from a technology perspective (e.g. TRL), but also addressing other parameters that play a role in the uptake of Innovation (e.g. IRL, CRL, MRL, SPRL, SRL)
- Development of a composite maturity assessment framework that:
 - Is tailored to the specific context of application (i.e. Civil security);
 - Provides commonly agreed definitions;
 - Incorporates tools that allow a holistic, quantitative and reliable measurement / assessment of the readiness of innovative security technologies.



2021-SSRI-01-01: A maturity assessment framework for security technologies

- A maturity assessment framework at the service of EU-funded security R&I:
 - Allowing guided and/or self-assessment;
 - Open acces for use to EU-funded security R&I projects;
 - Extensive validation based on real EU-funded R&I outputs;
 - Contribute with validation results and analytics to the work of bodies or initiatives of the EU-funded security R&I ecosystem (e.g. CERIS, Networks of Practitioners – Knowledge Networks, Innovation Labs at EU Agencies)
- Proposal for continuity of operations beyond the duration of the Project.

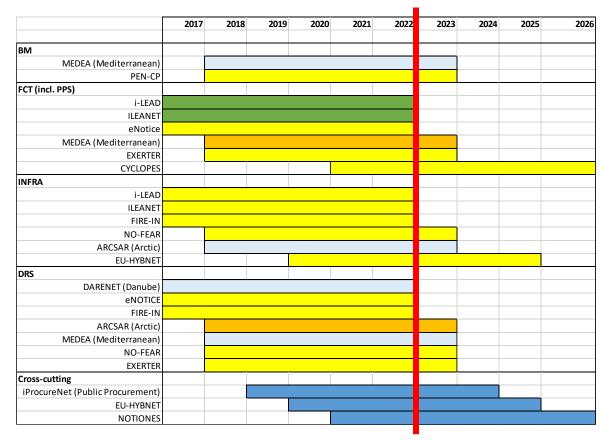


Topics	Type of Action	Budgets (EUR million)	Expected EU	Number of projects	
		2021	contribution per project (EUR million)	expected to be funded	
HORIZON-CL3-2021-SSRI-01-02	CSA	4,00	Around 2,00	2	

- Expected outcome
 - Enhanced analytical capacity to support the programming of EU-funded security research and capacity building funds through a periodic and timely evidence-based policy feedback
 - Periodic aggregated and consolidated view of capability needs and gaps, technological and R&I landscape, including trends and best practices
 - More systematic assessment, validation and exploitation of security R&I outcomes
 - Identification of areas requiring standardisation and/or certification, as well as training
 - Enhanced cooperation among security ecosystem stakeholders (policy makers, security practitioners, industry, researchers and citizens)



- Pan-European Networks of Practitioners H2020: Practitioners (end-users) in the same discipline and from across Europe 1) to **monitor R&I** with a view to **recommending the uptake** or the industrialisation of results, 2) to express **common requirements** for innovations that could fill capability gaps, 3) to indicate **priorities** as regards areas requiring more **standardisation**.
- Collect, aggregate, process, disseminate and exploit existing knowledge and contribute to expected outcomes.
- Build on strong points of H2020 NoPs and achieve a better alignment with the EU security R&I policy framework:
 - Purpose: Support to an evidence-based security research programming with a view on an increased uptake of innovation.
 - **Harmonisation**: Clearer definition of expected outcomes
 - Rationalisation: Less networks better aligned with the four main policy areas (INFRA, DRS, FCT, BM)



- Dissemination and exploitation of findings as a key for success:
 - Contribute, every 6 or fewer months, to working groups chaired by the European Commission and/or EU Agencies (Eligibility condition)
 - CERIS Thematic Working Groups, Innovation labs of EU Agencies, etc. → Check the right timing!!
 - Each proposal must include a work package to disseminate their findings, including an annual workshop or conference (Eligibility condition)
- Knowledge and skills:
 - Participation as beneficiaries of end-user authorities with a recognised mandate in the areas addressed by the network from at least 3 different EU Member States or Associated Countries is mandatory (Eligibility condition)
 - Ensure representativeness of communities of interest and a balanced coverage in terms of knowledge and skills of the different knowledge domains required to face the challenge, including security operations, technologies, research & innovation, industry, market, etc.

- Collaboration stakeholders beyond the consortium partners:
 - Each proposal should include a plan, and a budget amounting at least 25% of the total cost of the action to carry out activities involving industry, academia and other providers of innovative solutions outside the consortium.
 - Beneficiaries may provide financial support to third parties in the form of prizes (Specific conditions).
 - Recommended to build as much as possible on the existing Networks of Practitioners, and to seek cooperation when the NoP projects are still ongoing.
- Thematic areas addressed only one KN per area can be funded
 - Option A: Border Security
 - Option B: Resilient Infrastructure

(Specific conditions)



2021-SSRI-01-03: National Contact Points (NCPs) in security and cybersecurity

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per	Number of projects expected to be funded
		2021	project (EUR million)	expected to be fullded
HORIZON-CL3-2021-SSRI-01-03	CSA	2,50	Around 2,50	1

- Expected outcome
 - Improved and professionalised NCP service thereby helping simplify access to HE calls
 - Harmonised and improved trans-national cooperation between NCPs, with the engagement of NCPs from associated partners in third countries and the EEN;
 - Policy feedback in support to EU-funded security research programming enabled by a seamless integration of the national, regional and local dimensions
 - Systematic assessment of the needs of the stakeholders involved in security and Cybersecurity research projects and programmes and assessment of their impact to the research community;
 - Collaboration with the future National Coordination Centres created through the Cybersecurity Competence Centre and Network Regulation (Regulation (EU) 2021/887);

2021-SSRI-01-03: National Contact Points (NCPs) in security and cybersecurity

- Ambassadors for Horizon Europe, perceived as true and impartial partners of the EC Services and its Agencies;
- Support structures that have become essential in implementing the Framework Programmes;
- Highly support professional services of knowledge and expertise; they provide information and on-the-ground advice to potential applicants and beneficiaries, through the project life cycle;
- Facilitators of access to funding opportunities and of visibility of impact and research results;
- Enablers of contacts with strategic actors, breaking geographical silos;
- The activities of the NCP Network should be tailored according to the nature of the area in the WP and the priorities of the NCPs concerned;

2021-SSRI-01-03: National Contact Points (NCPs) in security and cybersecurity

Considerations

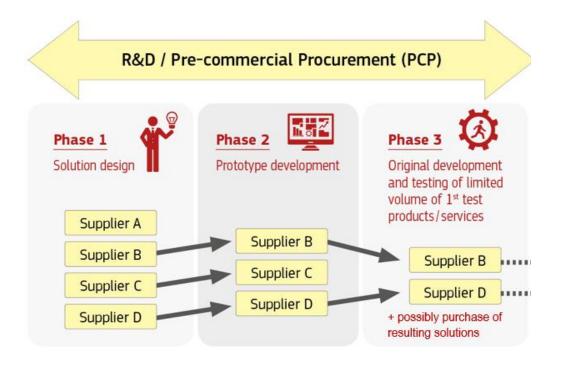
- Applicants must be Horizon Europe national support structures (e.g. NCP) responsible for Cluster 3 and officially nominated to the EC from an EU MS or an Associated Country;
- The project consortium should have a good representation of experienced and less experienced NCPs;
- Where relevant, synergies should be sought with the Enterprise Europe Network to organise matchmaking activities; such activities should also link up potential participants from widening countries;
- The project proposal to be funded should cover a wide range of activities related to
 Horizon Europe and address issues in the thematic areas specific to the Cluster "Civil
 Security for Society;

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per	Number of projects expected to be funded
		2021	project (EUR million)	expected to be fullded
HORIZON-CL3-2021-SSRI-01-04	PCP	6,00	Around 6,00	1

- Expected outcome
 - An identifiable community of EU first responders with common user/functional needs for innovative technology solutions for situation awareness in the field of civil protection
 - Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes for situation awareness in the field of civil protection that meet the needs of the EU user community
 - Improved delineation of the EU market (including demand and supply) for situation awareness systems in the field of civil protection



• **Pre-Commercial Procurement** – Procurement of R&I services to steer the development of solutions towards concrete public sector needs, whilst comparing/validating alternative solution approaches from various vendors



Background info on Pre-Commercial Procurement



iProcureNet 2021 Conference (presentations)



PCP/PP workshop (<u>video</u> + <u>presentations</u>)



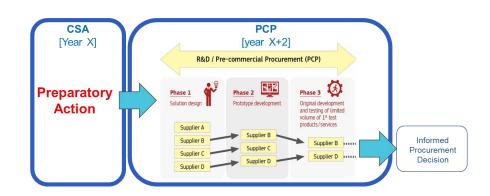
How to prepare a successful innovation procurement proposal (video)

European Commission

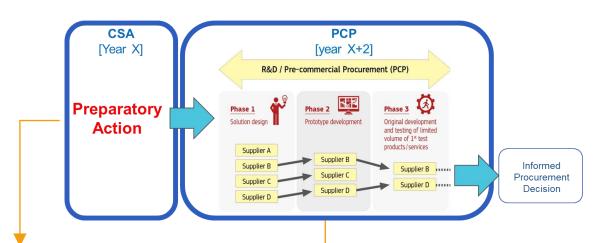
- Innovation Procurement in FP7 and H2020
 - Assessment of PCP instrument for security (<u>link</u> to public report)



- Innovation Procurement in Horizon Europe
 - 2 steps process: CSA + PCP → Reduced risk and improved credibility of PCP proposals
 - Clearer indications but not prescriptive
 - General simplifications helping also less experienced procurers: Less red tape, more guidance, simpler IT supported reporting and payment.







SEC-02-DRS-2016 - Situational awareness systems to support civil protection preparation and operational decision making.





- Proposals should give continuity to the work initiated under topic SEC-02-DRS-2016, but what really matters is to demonstrate:
 - A pertinent challenge
 - End-users committed to carry out a PCP action
 - Explored market (demand and supply)
 - A clear PCP tendering process
 - Commitment to pursue exploitation of results



- Indications on PCP tendering process (e.g. Directive, conflict of interest, societal aspects, intellectual property, data protection)
 - NEW Commission Guidance on Innovation Procurement C(2021) 4320, 18/06/2021
- Indications on PCP contract implementation (e.g. preparation stage, competitive development, phases, uptake strategy)
- Specific conditions
 - This topic requires the participation of at least **3 relevant end-user organisations** and **3 public procurers** from 3 different EU Member States or Associated Countries.
 - One organisation can have the role of end-user and public procurer simultaneously, both counting for the overall number of organisations required for eligibility.
 - The specific conditions for actions with PCP/PPI procurements in **section H of the General Annexes** apply to grants funded under this topic.
 - TRL 6-8 to be achieved by the end of the project.



Actions with as 'primary aim' the implementation of PCP/PPI procurement by a transnational buyers group (PCP/PPI procurement cost \geq 50% action budget)



NEW

PCP Actions (max 100% funding rate)

Fund actual PCP (1 joint PCP procurement/action) + related activities*

* To prepare, manage and follow-up the PCP/PPI procurement + embed the PCP/PPI in a wider demand side context (e.g. to test / label / certify / standardise solutions, prepare follow-up procurement, awareness raising and training)

Applicable rules and guidance



How to prepare a successful innovation procurement proposal



PCP and PPI in Horizon Europe: The rules of the game – funding conditions



2021-SSRI-01-05: Security research techs. driven by active civil society engagement

Topics	Type of Action	Budgets (EUR million)	Expected EU	Number of projects	
		2021	contribution per project (EUR million)	expected to be funded	
HORIZON-CL3-2021-SSRI-01-05	RIA	2,00	Around 2,00	1	

Expected outcome

- Policy-makers, security practitioners, research community implement security technological solutions and policies that fulfil both societal and legal requirements, such as inclusiveness, accessibility, universal design, proportionality, ethics;
- Security practitioners and citizens have the necessary skills and knowledge on the use of the new technologies being produced, as well as their impact on the society;
- State and non-state actors base their decision making on assessing negative societal impacts of security research outputs (e.g. risks of ill-intended use);
- Security practitioners, the research community and policy-makers build upon existing knowledge on lessons learned and best practices, whilst respecting and promoting fundamental rights.

2021-SSRI-01-05: Security research techs. driven by active civil society engagement

Scope:

- Evaluate the impact of security research products to the society by taking stock of technological solutions through methodologies that allow citizens genuine participation, including vulnerable groups;
- Demonstrate awareness of the risks that potentially build biases into automated systems so as to identify best solutions for relevant functionalities;
- Improve knowledge on social, economic and political contexts that may create security problems through societal development plans;
- Achieve behaviour change through education, simulation, training modules on human and societal factors to override human misjudgement, lack of compliance or understanding;
- Enhance the effectiveness of innovations by inspiring socially acceptable design for societal transformation (e.g. desirability, directionality, ethicalness, etc.)

2021-SSRI-01-05: Security research techs. driven by active civil society engagement

Considerations:

- Proposal's consortia should comprehend a great range of expertise (e.g. industry, citizens' representatives, Social Sciences and Humanities experts) and knowledge in a balanced way → Ensure a multidisciplinary approach;
- Proposals' consortia are encouraged to cooperate closely with the Networks of Practitioners, funded under H2020 Secure Societies WPs, if relevant results on impact could be obtained;
- Proposals could be linked to finished or ongoing projects which have developed Societal Readiness Level Tools; some examples for inspiration are mentioned in the WP;
- Beneficiaries may provide financial support to third parties in the form of prizes up to 60k€.







EU Innovation and Industry for Security



Horizon Europe Strategic Plan Cluster 3
"Civil Security for Society"



EU Funding and Tenders Portal

Thank you!

HorizonEU #EUsecurityResearch

