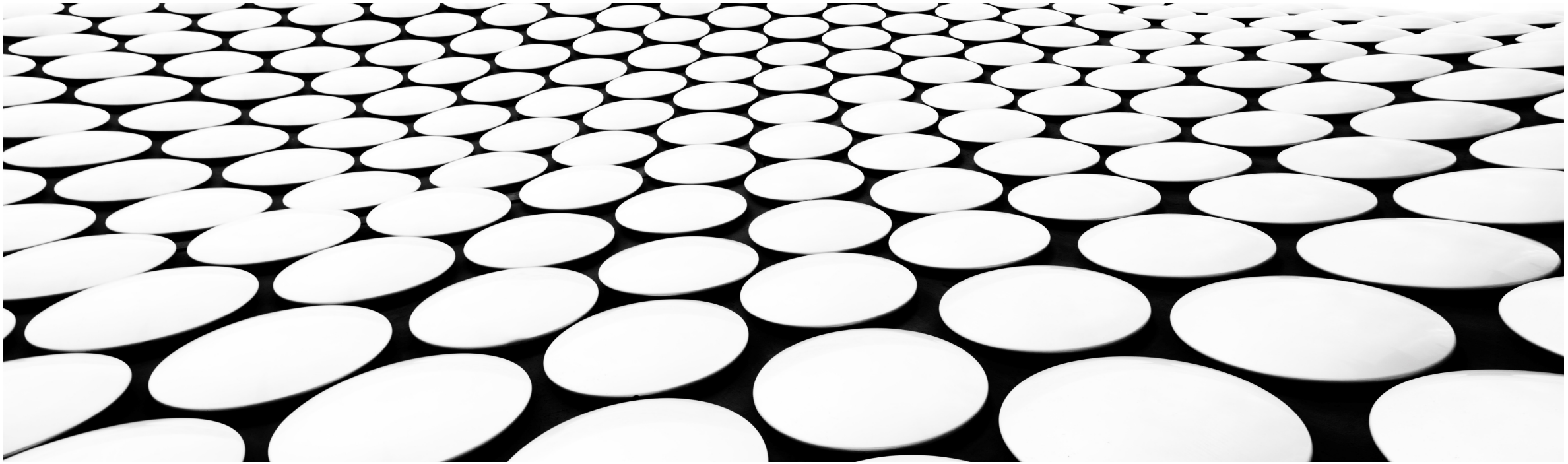
CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

ENTERPRISE IRELAND

HORIZON EUROPE: CYBERSECURITY IN 'CIVIL SECURITY FOR SOCIETY'

BY MICHAEL MURPHY PHD | ENTERPRISE IRELAND | 10TH JUNE 2021



CONTENTS

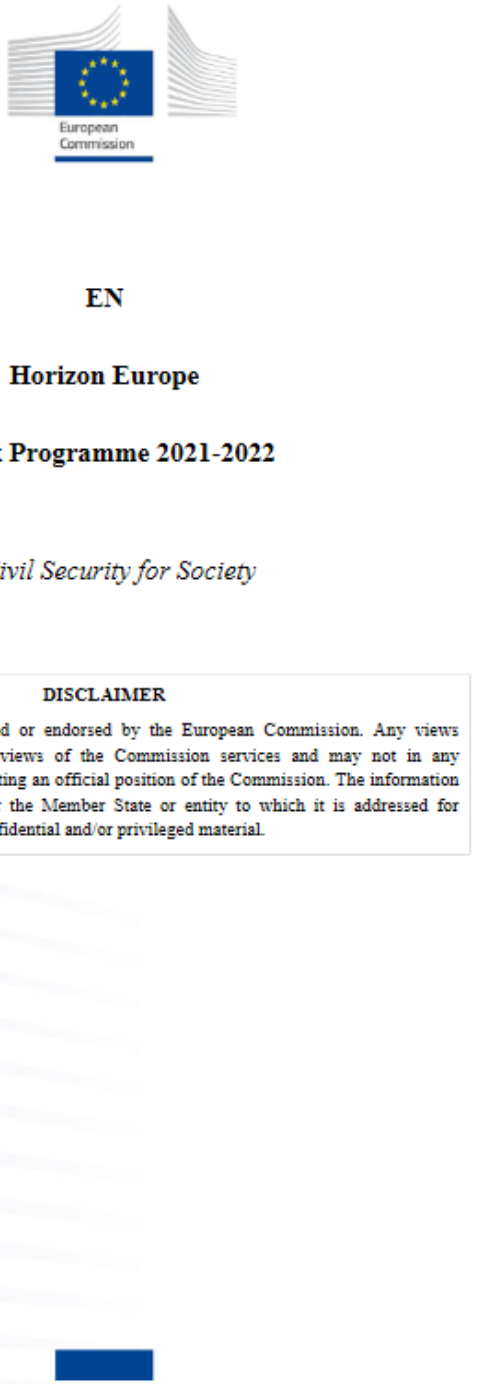
CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

ENTERPRISE IRELAND

1. WHERE TO START?

WORK PROGRAMMES

- Work programmes describe the overarching aims and give the menu of topics to be funded as well as specifying various rules. A close to final draft 'Civil Security for Society' Work Programme can be downloaded from https://ncpflanders.be/storage/media/86/WP-Cluster3-Civil-Security-for-Society.pdf
- Intending applicants are using this draft to plan their consortium proposals but be sure to use the final EC Work Programme once it's published on 30th June 2021.



EN

Horizon Europe

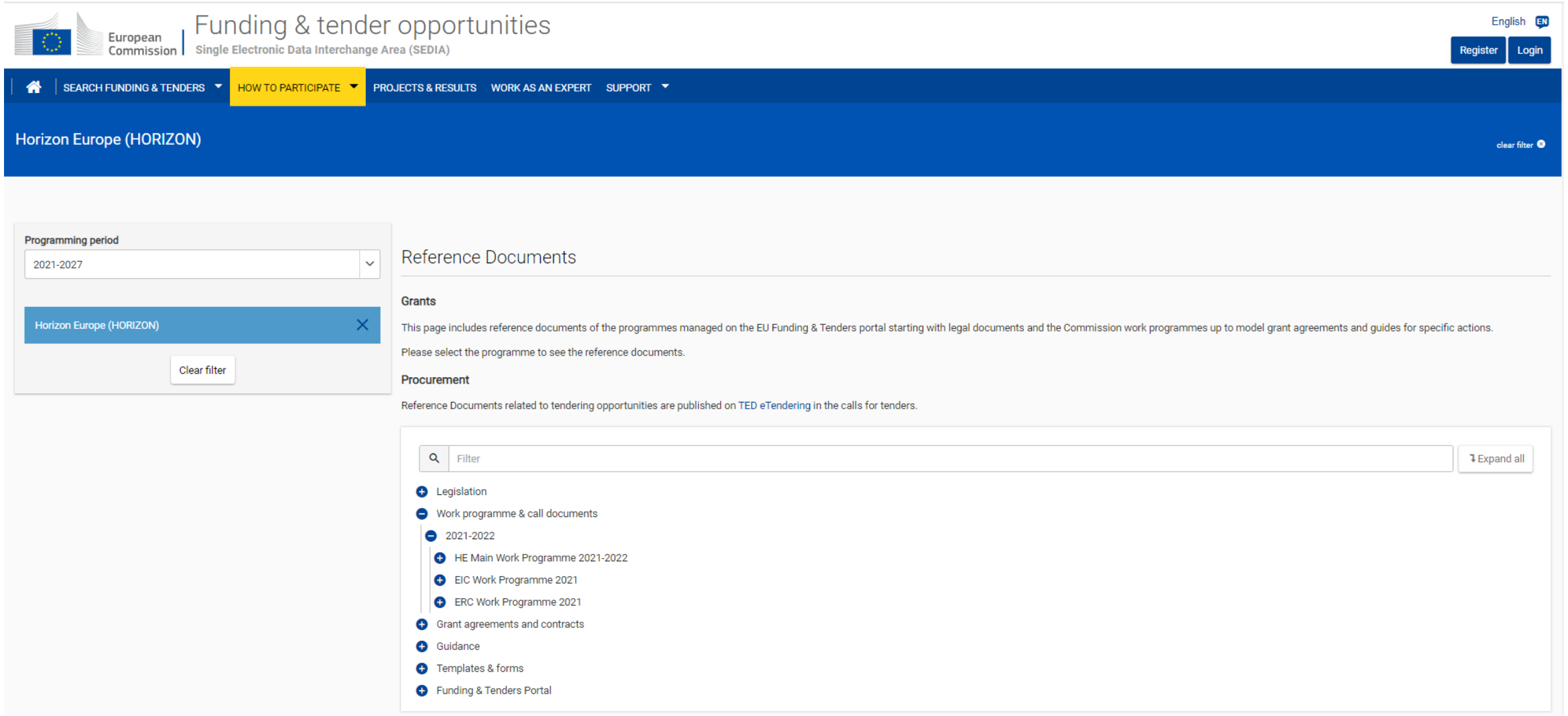
Work Programme 2021-2022

6. Civil Security for Society

DISCLAIMER

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and may contain confidential and/or privileged material.

THE FUNDING AND TENDERS PORTAL



https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/reference-documents

THE CLUSTER 3 'CIVIL SECURITY FOR SOCIETY' WORK PROGRAMME - IMPACT AREAS AND DESTINATIONS 2021-2022

The Cluster 3 work programme 2021-2022 has six destinations (key areas) below which contribute to four expected impact areas of the Horizon Europe Strategic Plan (see factsheet also):

1. Better protect the EU and its citizens against Crime and Terrorism (FCT)
2. Effective management of EU external borders (BM)
3. Resilient infrastructure (INFRA)
4. Increased Cybersecurity (CS)
5. A Disaster-Resilient Society for Europe (DRS)
6. Strengthened Security Research and Innovation (SSRI)

THE CLUSTER 3 'CIVIL SECURITY FOR SOCIETY' WORK PROGRAMME – STRUCTURE OF A TOPIC

HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement

Specific conditions	
Expected EU contribution per project	The EU estimates that an EU contribution of between EUR 3.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 11.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.
Technology Readiness Level	Activities are expected to achieve TRL 4 by the end of the project – see General Annex B.

Expected Outcome: Projects are expected to contribute to some of the following expected outcomes:

- Reinforced cybersecurity using AI technological components and tools in line with relevant EU policy, legal and ethical requirements.
- Increased knowledge about how an attacker might use AI technology in order to attack IT systems.
- Digital processes, products and systems resilient against AI-powered cyberattacks

The proposal should provide appropriate indicators to measure its progress and specific impact.

Scope: Artificial intelligence (AI) is present in almost every application area where massive data are involved. Understanding the implications and possible side effects for cybersecurity however requires deep analysis, including further research and innovation. On the one hand, AI can be used to improve response and resilience such us for the early detection of threats and other malicious activities with the aim to more accurately identify, prevent and stop attacks. On the other hand, attackers are increasingly powering their tools by using AI or by manipulating AI systems (including the AI systems used to reinforce cybersecurity).

The proposed actions should develop AI-based methods and tools in order to address the following interrelated capabilities: (i) improve systems robustness (i.e. the ability of a system to maintain its initial stable configuration even when it processes erroneous inputs, thanks to self-testing and self-healing); (ii) improve systems resilience (i.e. the ability of a system to resist and tolerate an attack, anticipate, cope and evolve by facilitating threat and anomaly detection and allowing security analysts to retrieve information about cyber threats); (iii) improve systems response (i.e. the capacity of a system to respond autonomously to attacks, thanks to identifying vulnerabilities in other machines and operate strategically by deciding which vulnerability to attack and at which point, and by deceiving attackers; and to (iv) counter the ways AI can be used for attacking. Advanced AI-based solutions, including machine learning tools, as well as defensive mechanisms to ensure data integrity should also be included in the proposed actions. Proposals should strive to ultimately facilitate the work of relevant cybersecurity experts (e.g. by reducing the workloads of security operators).

Regarding the manifold links among AI and cybersecurity, privacy and personal data protection, applicants should demonstrate how their proposed solutions comply with and support the EU policy actions and guidelines relevant to AI (e.g. Ethics Guidelines for Trustworthy AI[83], the AI Whitepaper[84], EU Security Strategy[85] and the Data Strategy[86]). Proposals should foresee activities to collaborate with projects stemming from relevant topics included in the Cluster 4 "Digital, Industry and Space" of Horizon Europe. Generally, proposals should also build on the outcomes of and/or foresee actions to collaborate with other relevant projects (e.g. funded under Horizon 2020, Digital Europe Programme or Horizon Europe).

Proposals should strive to use, and contribute to, European relevant data pools (including federations of national and/or regional ones to render their proposed solutions more effective. To this end, applicants should crucially strive to ensure data quality and homogeneity of merged/federated data. Applicants should also identify and document relevant trade-offs between effectiveness of AI and fundamental rights (such as personal data protection). Moreover, privacy in big data should also be addressed.

Key performance indicators (KPI), with baseline targets in order to measure success and error rates, should demonstrate how the proposed work will bring significant progress to the state-of-the-art. All technologies and tools developed should be appropriately documented, to support take-up and replicability. Participation of SMEs is encouraged.

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

ENTERPRISE IRELAND

2. CYBERSECURITY AND CYBERCRIME IN CLUSTER 3 'CIVIL SECURITY FOR SOCIETY'

DESTINATION 4 – INCREASED CYBERSECURITY – EXPECTED IMPACT

- *"Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats."*

CALL: INCREASED CYBERSECURITY 2021

- CS01 - Secure and resilient digital infrastructures and interconnected systems
  - HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity
- CS02 - Hardware, software and supply chain security
  - HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices
- CS03 - Cybersecurity and disruptive technologies
  - HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement
- CS05 - Human-centric security, privacy and ethics
  - HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

CONDITIONS FOR THE 2021 CALL – INDICATIVE BUDGETS

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[93]	Number of projects expected to be funded
		2021		
Opening: 30 Jun 2021 Deadline(s): 21 Oct 2021				
HORIZON-CL3-2021-CS-01-01	RIA	21.50	3.00 to 5.00	5
HORIZON-CL3-2021-CS-01-02	RIA	18.00	3.00 to 5.00	4
HORIZON-CL3-2021-CS-01-03	RIA	11.00	3.00 to 4.00	3
HORIZON-CL3-2021-CS-01-04	RIA	17.00	3.00 to 5.00	4
Overall indicative budget		67.50		

[93] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

CALL: INCREASED CYBERSECURITY 2022

- CS01 - Secure and resilient digital infrastructures and interconnected systems
  - HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures
- CS02 - Hardware, software and supply chain security
  - HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components
- CS03 - Cybersecurity and disruptive technologies
  - HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography
- CS04 - Smart and quantifiable security assurance and certification shared across Europe
  - HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

CONDITIONS FOR THE 2022 CALL – INDICATIVE BUDGETS

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[100]	Number of projects expected to be funded
		2022		
Opening: 30 Jun 2022 Deadline(s): 16 Nov 2022				
HORIZON-CL3-2022-CS-01-01	IA	21.00	4.00 to 6.00	4
HORIZON-CL3-2022-CS-01-02	RIA	17.30	3.00 to 5.00	4
HORIZON-CL3-2022-CS-01-03	IA	11.00	3.50 to 6.00	2
HORIZON-CL3-2022-CS-01-04	IA	18.00	3.00 to 5.00	4
Overall indicative budget		67.30		

[100] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

DESTINATION 1 - BETTER PROTECT THE EU AND ITS CITIZENS AGAINST CRIME AND TERRORISM – SUBSECTION FCT06: CITIZENS ARE PROTECTED AGAINST CYBERCRIME

- FCT06 – Citizens are protected against cybercrime (€6M)
  - HORIZON-CL3-2021-FCT-01-11: Prevention of child sexual exploitation (RIA – €3M)
  - HORIZON-CL3-2021-FCT-01-12: Online identity theft is countered (RIA – €3M)

- Under Specific Conditions:
  - The topic on '*Prevention of child sexual exploitation*' requires the active involvement, as beneficiaries, of at least 2 Police Authorities and at least 2 Civil Society Organisations (CSOs) from at least 3 different EU Member States or Associated countries.
  - The topic on '*Online identity theft is countered*' requires the active involvement, as beneficiaries, of at least 3 Police Authorities from at least 3 different EU Member States or Associated countries.

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

ENTERPRISE IRELAND

3. PARTICIPATION AND EVALUATION

YOU'VE IDENTIFIED A TOPIC – HOW TO PARTICIPATE?

Will you write your own proposal?

- In general, this is a significant endeavour that should not lightly be undertaken
- Start early – at least 6 months in advance of the proposal submission deadline is a rule of thumb
- If you're inexperienced then you should gather experienced partners willing to assist you

Can you prompt someone else to coordinate with you offering strong support?

You want to partner in somebody else's proposal - how do you identify a consortium in order to participate?

- Tap your existing networks
- Consult your national contact point
- Subscribe to relevant circulation lists including those of your national contact point
- Attend brokerage events
- Register on brokerage websites

THE EVALUATION PROCESS

- The evaluation process is well explained here https://www.youtube.com/watch?v=IIcm7zoEHLs

4. SUMMARY

- The Work Programmes and Funding & Tenders Portal are a starting point to identify opportunities
- Before you embark on a proposal (especially if you will coordinate), you should gauge your chances of winning
- Consult your national contact point, use your existing networks, attend and present at brokerage events, sign-up to relevant circulation lists, attend training events
- The cybersecurity topics are attractive because the EC funds multiple proposals under each topic
- The cybercrime topics likely will fund only one proposal each and applicants need to attract police authorities and others to their proposal and find a meaningful role for them
- There will be cybersecurity opportunities across Horizon Europe, under the EDF, and elsewhere, not only in Cluster 3

THANK YOU

Michael Murphy

Enterprise Ireland

Eastpoint Business Park

Dublin 3

Email: michael.murphy@enterprise-ireland.com