Q&A from the Secure Societies Info Day 13/14 MARCH 2019 in Brussels

Part 2: Questions on the SME instrument, the Security Union, on the topics for the SEC, INFRA and DS calls and the SEREN 4 services

5. Questions on the SME instrument

5.1: Can an entrepreneur submit a proposal for the SME instrument phase 1 or 2 if he/she has not yet created the legal entity?

No. One of the key eligibility conditions is that the applicant is a for-profit SME (including newly created companies and start-ups). For the EU definition of SME please consult this link.

5.2: May a SME, after participation in the SME Instrument, be acquired by a non-EU (e.g. a US) company?

There is no clause preventing the takeover by a non-EU actor after the end of the contract.

5.3: A recently created start-up might have difficulties to get a positive rating in the Financial Viability Check (FVC) by the EU. Can it nevertheless participate in the SME instrument?

Yes. In the case of a mono-beneficiary projects (i.e. participation of a single SME), the FVC is not required. For multi-beneficiary projects it is required only for the coordinator but not for the other participants.

5.4: Is it true that the calls for the SME Instrument Phase 1 will be discontinued in 2019?

Yes, the calls for the SME instrument Phase 1 will be discontinued after the September 5 deadline. For latest information regarding the deadlines for submission under the SME Instrument Phase 1 or 2 please consult the Funding & tender opportunities.

6. Questions on Security Union

6.1: How does the Focus Area on Security Union relate to the defence calls? Are the defence calls included in the cross-fertilisation of research?

The Focus Area 'Boosting the effectiveness of the Security Union' includes calls and topics only under Horizon 2020, and so all activities will have an exclusive focus on civil applications. However, applicants should also read the heading "Possible synergies with

defence research" which is to be found in the introduction of the Work Programme 2018-2020. In this paragraph, it is clearly stated that: "Where necessary, actions should clearly demonstrate how they complement and do not overlap with actions undertaken under the Preparatory Action on Defence Research."

6.2: Do the defence calls use the same funding portal?

The Commission adopted the Financing Decision for the PADR 2019 Calls for Proposals: https://ec.europa.eu/growth/content/preparatory-action-defence-research-description-2019-topics_en.
Soon after the adoption of the above Decision, the calls have been published, thanks to the European Defence Agency, onto the Funding and Tender Opportunities Portal – Pilot Projects & Preparatory Actions (PPPA).

7. Questions on the SEC call (BES, DRS, FCT, GM)

A: Border and External Security (BES)

7.1: For SU-BES02-2018-2019-2020, Sub-topic 3: [2019] *"Security on-board passenger ships",* is there any official definition for "passenger ship"? For example, would this include ferries?

The topic refers to "border and external security" (and not to the protection of critical infrastructures). Therefore, any threats/risks considered should originate outside of the EU or should relate to the crossing of borders. The reference to passenger ship addresses threats/risks, which are associated to the flow of people rather than to the flow of goods. Ferries crossing international borders could also be included.

According to the country, the authorities, which have the mandate to ensure security, may vary and may include customs and port authorities. As for meeting the additional admissibility and eligibility conditions, the proposal must therefore give sufficient evidence that the practitioners within the consortium have indeed the legal basis of responsibility regarding the security on-board passenger ships.

B: Disaster Resilient Societies (DRS)

7.2: The SU-DRS03-2019-2020: *"Pre-normative research and demonstration for disaster-resilient societies"* mentions that complementarity with EDA-funded projects should be targeted. Should therefore project proposers include EDA into the consortium?

The sub-topic 2: [2019] Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies) mentions indeed "*complementarity of proposed activities with activities supported by EDA in the CBRN-E area should be described comprehensively*". This does not mean that EDA should be included in the consortia. Applicants should demonstrate an awareness of the activities supported by the EDA in the CBRN-E area and how their submitted proposal under topic DRS03 complements possible activities by EDA.

Applicants can get information on the activities of EDA consulting the following web sites:

https://www.eda.europa.eu/what-we-do/activities/activities-search/cbrn-joint-investment-programme

https://www.eda.europa.eu/what-we-do/activities/activities-search/captech-cbrn-and-hf

https://www.eda.europa.eu/info-hub/events/2017/03/07/default-calendar/workshop-on-space-and-cbrne-threats

7.3: The topic description of SU-DRS04-2019-2020: *"Chemical, biological, radiological and nuclear (CBRN) cluster"* makes reference to the project ENCIRCLE. Where can we find information on this project?

The mentioned technology and innovation catalogue of ENCIRCLE can be consulted in the "*Topic conditions and documents*" section of DRS04 on the Funding & tender opportunities portal (cf. direct link).

Further relevant information on ENCIRCLE can be found on the project's website under http://encircle-cbrn.eu/related-projects-2/eu-cbrne-projects/eda/

7.4: For SU-DRS02-2018-2019-2020 is it mandatory to foresee international cooperation with Japanese or Korean research centres? Will there be some EU support for them?

The cooperation with Japanese and/or South Korean research centres is not mandatory. The call mentions: "international cooperation according to the current rules of participation is encouraged (but not mandatory)".

Very importantly, Japanese and Korean organizations that wish to participate should contact their national agencies (links are provided in the topic text) and apply for national funding, as entities from these countries are funded by the EU only on an exceptional basis (cf. General Annexes, part A, for more information on exceptional funding).

7.5: To what extent should applicants under topic SU-DRS01-2018-2019-2020: *"Human factors, and social, societal, and organisational aspects for disaster-resilient societies"* focus on technologies?

Topic DRS01 focusses on *"human factors, social, societal and organisational aspects"*. The reference to technologies is about the way citizens will understand, accept and implement them, which is a matter of raising awareness and not of a technology development as such. The research targets mainly cultural changes, citizen risk awareness and involvement. The topic clearly states that "*Civil society organisations, first responders, (national, regional, local, and city) authorities are invited to propose strategies, processes and methods […] that should be tested with citizens and communities […] in checking and validating proposed tools, technologies and processes for disaster management*". The reference to technologies only relates to their validation (involving citizens) but this is not the main emphasis of the topic. For technology-oriented projects, the DRS02 call is more appropriate.

C: Fight against Crime and Terrorism (FCT)

7.6: Can you please specify what entities are considered as Law Enforcement Agencies (LEAs)? Would police forces, ministries of Interior and/or ministries of Justice be valid examples?

A LEA may be a police authority or any other law enforcement service in a Member States, acting at national, federal and/or regional levels, depending on the legal system of each Member State. They are responsible under national law for preventing and combating criminal offences, listed in Annex I of the EU Regulation 2016/794.

7.7: Within the topic SU-FCT01-2018-2019-2020: "*Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime*", may cyber-criminality also include the aspect of cyber-bullying?

As written in the study "Cyberbullying among Young People", bullying online may be classified as a cybercrime falling under the Budapest Convention on Cybercrime. Furthermore, bullying online could fall within the category of computer crimes according to the definition provided by 2000 Commission's Communication on cybersecurity. It defines a 'computer crime' as any crime involving the use of information technology – thus, it may include bullying online.

7.8: For proposals under topic FCT03-2018-2019-2020: *"Information and data stream management to fight against (cyber)crime and terrorism"*, may applicants address the misuse of cryptocurrencies?

Existing threat assessments (see, for instance, Europol's Internet Organised Crime Threat Assessment 2018) list criminal abuse of cryptocurrencies among the main cyber threats. If applicants wish to address this threat under topic FCT03, it is up to them to justify in the proposal how this threat fits in the overall context of the topic.

D: General Matters (GM)

7.9: Are military organisations considered as practitioners in the context of GM01-2018-2019-2020: "*Pan-European networks of practitioners and other actors in the field of security*"?

In the call text, the term "practitioner" refers to someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. In assessing their eligibility conditions, beneficiary organisations who take the role of practitioners shall be duly identified in the proposal, and their role and added value shall be clearly described and justified taking into account the scope of the call, the specific challenge and the scope of each topic. Defence organisations might be eligible for funding if the above conditions are duly addressed in the proposal. Regarding defence organisations, applicants shall also be aware of Article 19(2) of the Regulation 1291/2013 establishing Horizon 2020, which stipulates that: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications".

8. Questions on the INFRA call

8.1: Concerning the topic SU-INFRA01-2018-2019-2020: "*Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*" is there any reference list of Critical Infrastructures that can still be addressed by a proposal?

The topic description of SU-INFRA01 lists the critical infrastructures that applicants can address in their proposals. In order to cover the largest possible spectrum of installations and

to ensure minimum overlapping, new proposals should be complementary with respect to the already funded projects.

A list of infrastructures and specific installations already covered in the previous calls since 2016 and further information on the funded projects can be found under "*Topic Updates*" of INFRA01 on the Funding & tender opportunities portal (cf. direct link)

8.2: Concerning the topic SU-INFRA02-2019: "*Security for smart and safe cities, including for public spaces*" should applicants focus more on reducing the vulnerability of the soft target or on providing a holistic framework for cyber security?

There is no prescription on this. The focus of SU-INFRA02 is on the security for smart and safe cities, including security (protection) for public spaces. It is therefore by no means exclusively limited to cyber-related threats. Proposals should take due regard to the context/specific challenge described in the topic and address EU policy priorities in this field as outlined in the Action Plan to support the protection of public spaces. Proposals should ensure also to fully address the expected impact and respond in the best way to conditions and requirements described in the 'scope' section.

8.3: With regard to the topic SU-INFRA02-2019 "*Security for smart and safe cities, including for public spaces*" **should applicants address crowd and citizens' protection rather than protection of the city infrastructures?**

There is no prescription on how the proposals should address the challenge described in the topic; they must respond to the conditions and requirements mentioned in the 'scope' section. Nevertheless, proposals should have a clear reference to the policy context, most notably to the priorities identified in the Action plan to support the protection of public spaces. Applicants should take into account the expected impact as described in the topic and propose appropriate solutions that address such an impact.

9. Questions on the DS call

9.1: For the sub-topic SU-DS05a [2019]: *"Digital security, privacy and personal data protection in multimodal transport"*, does the concept of transport covers multimodality of goods and/or of people?

In principle, both aspects can be addressed; there is no prescription. Multimodality here suggests different types of transportation e.g. trains, airplanes, ships, vehicles used in the

provision of a supply chain service (e.g. container management, vehicle transfer) or in the movement of people. For example, a definition of multimodal transport:

"Multimodality" in the transport sector, or "multimodal transport" refers to the use of different modes (or means) of transport on the same journey.

The concept applies to both freight and passenger transport […]

For the DS05 topic, it is important to address the specific challenge in its complexity, as described in the topic, and take account of the policy context, i.e. the implementation of the NIS Directive where certain sectors/subsectors are identified as critical from the point of view of cybersecurity needs (e.g. energy, transport, banking, financial market infrastructures, health sector, etc.)

9.2: As regards the generic threats within the topic SU-DS05-2018-2019: *"Digital security, privacy, data protection and accountability in critical sectors"*, are these threats generic to all sectors or only to transport and health?

The topic description of DS05 states: *"Among the critical sectors mentioned in the NIS Directive (the footnote mentions Annex II of the NIS directive), 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."*

Generic aspects could apply to all sectors, and the project proposers should choose two sectors from Annex II of the NIS Directive, to treat these generic aspects (e.g. the loss of integrity is a generic threat in all sectors).

9.3: What are the relevant policies to be kept in mind when preparing a proposal under SU-DS03-2019-2020: *"Digital Security and privacy for citizens, and Small and Medium Enterprises and Micro Enterprises"*?

To have a good overview on the relevant policy context, applicants should refer to the introductory pages of the DS call and consult the indicated references. Among the most relevant references we can quote the Cybersecurity Act, the GDPR, the NIS directive and the eIDAS.

10. Questions on SEREN 4 services

10.1: Which quality parameters are you using when approving or disapproving input in SEREMA?

Concerning quality criteria within the SeReMa partner search tool, including also high quality of entries within the tool, all Security NCPs shall check their national entries. If a profile needs to be improved, the Security NCPs will contact the client (give them a call or send them an e-mail) and discuss which parts need to be improved.

The Security NCPs will receive an e-alert after a researcher or an organisation of their country has added a profile and will check all data given and contact the researchers, if more information is needed.

Following approval, the profile will be published in the SeReMa database.

In addition, as a backup, the two administrative entities of the SeReMa tool (task leader and work package leader) will have access to all profiles in the database (both published and unpublished) and will monitor the progress of the profile. They will be in touch with the local NCP - if appropriate - to prompt them to check their country profile.

Please find below a table with further details.

Quality Criteria	**Evaluation Questions**
Content	1. Is the template complete? 2. Are the links accurate? 3. Does the organisation really exist? 4. Is the information relevant? 5. Is the organisation experienced in security research or related research fields (according to template)? 6. Is the profile used by a company, which provides services?
Error check	a. Are there any grammatical errors, incomplete records or other "dirty data"? b. Are there faulty records identified?
• **If any of the criteria above are not fulfilled, please contact the person who filled in the profile and indicate what is missing and what should be changed.** • **If the data is not correct or missing, do not approve the profile!**	