Q&A Infoday Secure Societies March 12 and 13

FIRST DAY (12 March 2018)

Q: May an international organization, such as NATO, receive funding?
A: International organizations (IOs), such as NATO, Interpol or United Nations bodies, will only be eligible for funding - in the absence of a bilateral scientific and technological agreement or any other arrangement between with the EU – if the Commission deems the participation of the entity *essential* for carrying out the action. This could be based for example on its unique competences, access to data, geographical areas or infrastructures. In practice, the Commission will follow the evaluators' opinion on this point which will be discussed during the evaluation at the consensus and panel meeting.

Q: Can an entity which is a member of an association participating in the action, contribute to the action as linked third party?
A: According to Article 14 of the Grant Agreement, in order to be considered as a linked third party, an entity must be either affiliated to the beneficiary or have a legal link which is not limited to the action. Therefore, if an association is a beneficiary of a project, one of its members could in principle be considered as a linked third party.

Q: If there are even more layers to the above situation (an entity that is part of a national association that is part of a European association). Can this entity be considered a linked third party to the European association?

In order to be considered as a linked third party, an entity must be either affiliated to the beneficiary or have a legal link which is not limited to the action. When the involvement of third parties is requested, a case-by-case analysis is always needed; therefore the Commission is unable to respond to specific questions prior to this analysis.

Q: If an entity is coordinator or beneficiary of an action selected for funding with a grant amount higher than its turnover, may the Commission refuse to accept its participation?
According to Article 8 of the Grant Agreement beneficiaries must have the appropriate (technical, human and financial) resources to implement the action. As a consequence, before granting funding, the Commission may check the financial viability of the entity. In particular, unless exempted by its legal status, coordinators in actions with funding levels equal or superior to EUR 500,000 have to demonstrate their financial health on a number of key indicators based on recent financial data. In case of weak financial health the Commission is obliged to take the appropriate measures (e.g. impose change of coordinator, etc.). More detailed information can be found under this link.

Q: Can an entity located in a high-income country such as the USA or Canada deliver in-kind contribution against payment?
A: Entities which are not established in countries listed as being eligible in Annex A of the Work Programme, are only eligible for funding if the Commission deems their contribution as essential for carrying out the action or if funding for such participants is provided for under a bilateral scientific and

technological agreement or any other arrangement between the EU and the third country. This also applies to contributions from third parties.

Q: What is the purpose of the involvement of the ethics experts?

A: The ethics experts are independent experts, who are not involved in the scientific evaluation, and possess a specific expertise in ethical issues. Their task is to evaluate whether the consortium has sufficiently addressed any potential ethics issues in the proposal that might be raised during the implementation of the action. The experts may also propose further requirements have to be fulfilled to guarantee compliance with the ethical guidelines and relevant legislation.

SECOND DAY (13 March)

Q&A SME & FTI

Q: How many security-related projects have been funded over the past years in the SME Instrument and FTI?

A: Under FTI, about 3-4 projects out of 90. In SME Instrument, also 2-3 projects per cut-off date, which gives a similar number.

Q&A DS Call

Q: Who can apply for the H2020 Inducement Prize "online security - seamless personal authentication (authentication for all)"? Is it open to a consortium or to an individual? Could a mature solution, already being used in practice, be proposed?

A: The European Commission has published the Rules of Contest (RoC) for this Prize on the Participant Portal, please download them from there. Both individual applications and joint applications by a group of participants are admitted. In the latter case, the participants must appoint a 'lead participant' to represent them towards the Commission.

There are nine award criteria and a maximum score of 100 points can be obtained. The criterion "significant contribution to the state of the art" has the highest weight with a maximum of 23 points allocated. Hence, innovative approaches to authentication are requested. Applications will need to convince the jury also on other important aspects such as: usability and applicability, and compliance with privacy and data protection requirements. The five best applications will be invited as finalists for a hearing with the jury, where they will have to demonstrate their solution on a prototype running in an operational environment. Hence, the finalists should combine existing and new technologies/approach.

Q: Concerning topic SU-DS04-2018-2019-2020 on cyber-security in the Electrical Power and Energy System, does it also cover the cyber protection of gas networks?

A: This topic is restricted to electrical power and energy systems.

Q: The DS-05 topic addresses Digital security, privacy, data protection and accountability in critical sectors (as referenced in the NIS Directive) requiring to treat generic aspects of at least two sectors. Could you please elaborate this?

A: The applicants should indeed treat the generic aspects of at least two different critical sectors as listed in Directive on security of network and information systems (NIS Directive). Please note that it is required to treat specific aspects for one of the three critical sectors/domains mentioned as sub-topics - healthcare being the only one open in 2018 - by identifying specific vulnerabilities, propagation effects and counter measures, by developing and testing cyber innovation-based solutions and validating them in pilots/demonstrators.

Q: Are there any topics dedicated to research on block chain technology?

A: There are no specific topics dedicated to block chain, but there are definitely opportunities to include this emerging technology in a proposal. For instance, under topic SU-ICT-03, applicants are asked to build consortia that engage together in research, development and innovation in next generation industrial and civilian cybersecurity technologies with a specific focus on critical sectors including finance. If you think that the block chain technology should be addressed in this (or another) context, you can make your case and include it in the proposal.

Q&A Focus Area

Q: Where can applicants find information about previous- or currently-funded projects in order to avoid duplication and to better position their proposals under the open calls and topics of the Security Union focus area?

A: The entry point for any information on EU projects is via the CORDIS page on the Participant Portal. Using the search option you can easily find information on relevant EU projects.

Information can be also be obtained through the "Community of Users on Safe, Secure and Resilient Societies" (CoU) network where researchers, policy-makers and industry regularly meet and exchange views on project outcomes, end-user needs and relevant policy.

The European Commission is developing an IT tool with a query function that will allow the extraction of information about EU funded research projects. This tool aim is to make the relevant information more easily retrievable and will also cover projects funded under the Internal Security Fund.

Q&A CIP Call

Q: Among the critical infrastructures included under SU-INFRA-01-2018-2019-2020 the term "sensitive industrial sites and plants" is used. Could you please explain what "Sensitive industrial sites and plants" refers to under this topic?

A: "Sensitive industrial sites and plants" refers to facilities, installations or installation parts, not related with the other Critical Infrastructure (CI) types contemplated in this call, where incidents, failures or disruptions in their operations as a result of combined physical and cyber-attacks would entail serious damage to EU citizens' health and the environment or/and the collapse of essential sectors of our society.

Q: The SU-INFRA01-2018-2019-2020 topic description includes under the critical "energy infrastructure" as examples "power plants and distribution, oil rigs, offshore platforms". Is this list exhaustive or can applicants address other aspects of energy infrastructures?

A: The list is not exhaustive and proposals are welcome to consider other aspects of energy infrastructures. Although, please note that applicants are asked to minimize the overlap with previously funded projects under the H2020-CIP-2016-2017 call. For further information on this aspect please regularly consult the call and topic updates of SU-INFRA01-2018-2019-2020 on the Participant Portal.

Q&A DRS Call

Q: Do you expect a technology output from proposals submitted under the topic SU-DRS01-2018-2019-2020 "Human factors, and social, societal, and organisational aspects for disaster-resilient societies"?

A: The scope of this topic is centred on the human factors, and social, societal, and organisational aspects of the topic, however this may include the interrelation with existing or emerging technologies, such as communication technologies or social media.

Q: Is the inclusion of non-EU partners in the DRS topics beneficial or even mandatory, and how will it influence the evaluation?

A: There is no obligation in the DRS topics to have non-EU partners in the consortium. Participation of non-EU partners is always welcome when there is a clear added value. In the topic SU-DRS02-2018-2019-2020, participation of Japan and Korea is specifically mentioned due to ongoing dialogues with these countries, but involvement of partners from these countries is not an eligibility condition and proposals not involving partners from third countries will not be penalized. On the other side a well-designed proposal including the participation of partners from third countries could contribute to a higher impact through the exchange of best practices among the international consortia.

Q&A BES Call

Q: Concerning the topic SU-BES02-2018-2019-2020 "Technologies to enhance border and external security", are applicants expected to address all aspects mentioned under the chosen subtopic?
A: In principle, yes; it is up to the applicants to find the right balance between the different aspects.

Q&A FCT Call

Q: How should applicants to the subtopic 1 of SU-FCT01-2018-2019-2020 address the aspects of "trafficking of human beings and child sexual exploitation"?
A: Both aspects of this topic should be addressed in a balanced way. Regarding human trafficking, all victims of trafficking are concerned, not only child trafficking. Similarly, regarding child sexual exploitation, all victims of child sexual exploitation are concerned, not only victims of child sexual exploitation resulting from human trafficking.

Q: What is the target Technology Readiness Level (TRL) of the Research and Innovation Action (RIA) topic SU-FCT01-2018-2019-2020?
A: The topic description of SU-FCT01-2018-2019-2020 – focusing on human factors and social, societal and organisational aspects rather than on technology aspects – does not explicitly mention an expected TRL. In general, Research and Innovation Actions target a TRL of 4-6.

Q: Does topic SU-FCT03-2018-2019-2020 "Information and data stream management to fight against (cyber) crime and terrorism" focus on cyber and / or physical crime?
A: The topic requests improved capabilities of big data analysis designed to the needs of crime investigators, regardless if the crime is or will be committed in the virtual or the real world. Trends in cybercrime need to be properly addressed.

Q: The topic SU-FCT03-2018-2019-2020 makes reference to "soft targets", what is understood by this term?
A: The term "soft targets" is commonly used to designate relatively unprotected civilian sites, such as any crowded or open area. This stands in contrast with the critical infrastructures as addressed in the SU-INFRA01-2018-2019-2020 topic.