CEF TELECOM – 2020-2 CALLS FOR PROPOSALS

FREQUENTLY ASKED QUESTIONS

Cybersecurity – 26 October 2020 version

All information in blue has been added or updated since the previous version.

Commonly used abbreviations in this FAQ

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSP	Core Service Platform
DSP	Digital Service Provider
ENISA	European Union Agency for Network and Information Security
ISAC	Information Sharing and Analysis Center
MeliCERTes	EU-funded cooperation and information sharing platform for the Computer Security Incident Response Teams (CSIRTs)
NIS	Network and information systems
OES	Operator of Essential Services

1. What is the difference between this call and the 2019-2 Cybersecurity call?

The main differences between this year's call and the 2019-2 Cybersecurity call are as follows:

The current call has 4 different Objectives, which differ from the 2019 ones:

- Objective 1: Support for Operators of Essential Services (OES), National Competent Authorities, and Information Sharing and Analysis Centres (ISACs)
- Objective 2: Support to joint preparedness, shared situational awareness and coordinated response to cybersecurity incidents
- Objective 3: Support to the implementation of cooperation activities of the Second Biannual Work Programme of the NIS Cooperation Group (2020-2022)
- Objective 4: Support to cooperation and capacity building for cybersecurity certification in line with the Cybersecurity Act

Please note that each Objective targets different applicants. Applicants are therefore strongly advised to read carefully the eligibility requirements for each Objective in Section 6 "Eligible applicants".

2. Is there the obligation to form a consortium in order to submit a proposal?

A proposal **must** be submitted by a consortium **where explicitly indicated**, i.e. under Objective 3. Proposals submitted under this Objective must include national public authorities and/or national public bodies from at least two different Member States. Note that in this case the consortium must be transnational.

3. Is it possible to address several Objectives?

Each proposal can only address **one specific Objective** and the proposal should clearly specify which Objective is being addressed.

4. Is it possible to submit several proposals for the same Objective?

An applicant could submit multiple proposals for the same Objective. Given the differences among the Objectives, applicants are invited to check the eligibility criteria carefully under section 6 of the call text[1].

5. Is there a limit to the number of proposals that can be submitted by the same entity?

There is no limit to the number of proposals that can be submitted by the same company/entity.

6. Are any budget limitations applying to any of the objectives?

The total budget earmarked for the co-financing of projects under this call for proposals is estimated at €10.5 million.

Out of the total budget of €10.5 million, it is expected to allocate €1 million under Objective 3 and €1 million under Objective 4.

7. What level of detail are we expected to provide in our proposal for the technical items/equipment that we intend to purchase? For example, for a hardware platform should we specify all of the necessary equipment such as the servers, switches, etc.?

A summary list of major cost items should be provided in the proposal under the relevant activity description in application form part A. See the "Costs" section of the Guide for Applicants[2] for more information.

The proposal must clearly explain what the function of the equipment in the context of the project/activity is.

8. In view of the fact that under some Objectives applicants might develop/enhance their cybersecurity capacities, to what extent is it possible to subcontract activities to be carried out in the proposed action?

In line with the priorities and objectives of the call, in the proposed Action, emphasis must be put on strengthening in-house capacities of the applicants. In case subcontracting is foreseen for certain activities (e.g. provision of IT services), appropriate justification and transfer of knowledge from the contractor to the beneficiary has to be taken into account and described in the proposal.

Depending on the nature of the contractual relationship, a contract for the implementation of specific activities may be considered as procurement or subcontracting in accordance with Articles II.9 and II.10 of the model grant agreement. Please note that proposals involving subcontracting must explain (in particular in application form parts A3.1 and A3.2 and application form part D):

- What tasks will be subcontracted and for what reasons
- How the potential subcontractor will be selected in accordance with the provisions of the grant agreement (transparency, equal treatment and best value for money)
- The basis on which the estimated cost of subcontracting has been calculated

Having to subcontract implementation of some activities does not in itself affect the evaluation of proposal, however the elements listed above will be evaluated under the relevant award criteria

[1] Available on the call page: https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity

[2] Available on the call page: https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity

See section 13 of the CEF Telecom General FAQ[3] and section 4.2 of the Guide for Applicants for more information.

9. What kind of information is expected in the proposal to describe long-term sustainability of an action proposed under this call?

In section 3 of application form part D, applicants must address the Impact and Sustainability award criterion, as well as its sub-criteria. (See section 4.5 of the Guide for Applicants for more information).

Applicants must explain how their proposed Action will be sustained after its end, e.g. in terms of business case development (i.e. financial appraisal and evaluation). They should also consider other points such as:

- How will the results of the Action be embedded in the applicant's operations and organisation?
- How the proposed Action will be sustained, developed and scaled up without EU funding – and through funding sources other than the CEF?
- Is there a business model? How does the proposal fit in the applying organisation's financial strategy?
- Where applicable, are there details about successive stages of deployment and the corresponding target groups?
- How does the proposed Action create European added-value in the cybersecurity domain?
- How will the results be disseminated to key stakeholders in the domain, as relevant?
- How wider take-up of the Action's results will be ensured?

12. Can the European Union Agency for Cybersecurity (ENISA) assist applicants to the call?

ENISA may publicise and encourage participation in the call but it cannot be involved in preparing proposals, in line with the principles of transparency and equal treatment to all applicants.

13. Is there a recommended minimum or maximum grant amount per proposal?

No, there is no recommended minimum or maximum grant amount per proposal under this call.

14. Only public bodies, public authorities and industry stakeholders under the NIS Directive and Cybersecurity Act can submit proposals for generic services? Can a consortium be composed of private actors, exclusively, without the participation of public authorities?

With the agreement of the Member State(s) or EEA countr(y)ies concerned, international organisations, Joint Undertakings, or public or private undertakings or bodies can apply to this call. The call specifies additional eligibility requirements for each objective under section 6.a of the call text. If the concerned private undertakings or bodies do not meet the additional eligibility requirements per objective, they could apply as partners in a consortium with other entities that do meet those requirements. Please note that the activities proposed must be relevant to the call.

15. Can local authorities be involved in the call? How?

Yes, a local authority can apply to the call if it complies with the eligibility requirements outlined under section 6.1 of the call text, for example in Cybersecurity objective 1 if it has been identified by a Member State as an Operator of Essential Services (OES) in the context of the NIS directive. If it does not comply with any of the eligibility requirements indicated in section 6 of the call, it could apply as a partner in a consortium with other entities that do meet those requirements.

[3] Available at https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-cef-telecom-frequently-asked-questions

16. How is the indicative budget distributed per objective? Is there a budget defined for Objectives 1 and 2?

The total budget earmarked for the co-financing of projects under this call for proposals is estimated at €10.5 million.
Of the total budget of €10.5 million, €1 million is expected to be allocated under Objective 3 and €1 million under Objective 4. No specific budget allocation has been defined for Objective 1 and for Objective 2.

17. What is the average budget expected per project under Objectives 1 and 2? Or is there an indicative budget per partner?

The call does not specify any expected budget per proposal/partner. In any case, the requested funding must be proportionate to the objectives and scope of activities addressed by the proposal.

Each proposal can only address one objective.

18. Does CEF funding include the interconnection between cross-border local segments (companies) of a private multinational organisation for Cybersecurity purposes?

It depends on whether and how this interconnection would fit in one of the objectives of the call. For example, under Objective 1 an Operator of Essential Services (OES), identified or in the process of being identified, in line with the NIS Directive, can apply for improving internal capabilities to meet security and reporting requirements under national and EU legislation (see also Q15 above).

19. Which is the Technology Readiness Level (TRL) expected by the end of the project?

The call does not prescribe a specific TRL. However, note that CEF Telecom does not support research and innovation projects. As indicated in section 2.2 of the Work Programme, "CEF focuses on providing operational services which are ready to be deployed and which will be sustainable and maintained over time."

20. Is it possible to apply with a project which will be based fully on subcontracting costs (e.g. new servers, upgraded versions of existing IT systems)?

The call does not define a maximum percentage of the total eligible costs of a proposed Action which can be subcontracted, however the proposal must explain why the chosen approach is convincingly addressing the call.

If it is necessary to subcontract certain elements of the proposed Action or activities, this must be clearly identified in the application form, in particular application form parts A3.1 and A3.2 and application form part D.

Proposals involving subcontracting must justify:

- What tasks will be subcontracted and for what reasons
- How the potential subcontractor will be selected in accordance with the provisions of the grant agreement (transparency, equal treatment and best value for money)
- The basis on which the estimated cost of subcontracting has been calculated.

Having to subcontract implementation of some activities does not in itself affect the evaluation of the proposal, however the elements listed above will be evaluated under the relevant award criteria. For example, Objective 1, activity a) focuses on the improvement of OES capacities. In case subcontracting is foreseen for certain activities (e.g. provision of IT services), appropriate justification and transfer of knowledge from the contractor to the beneficiary has to be taken into account and described in the proposal.

Please refer to section 13 of the general FAQ for more information on subcontracting/procurement.

21. Which activities (services, hardware, paychecks, etc.) will be eligible without, and which will have to be procured through the public procurement process?

Please refer to section 13 of the general FAQ for more information on subcontracting/procurement.

Questions related to call objectives

22. Concerning Objective 1, can sector associations apply?

Section 6.1 of the call text explicitly provides that proposals submitted under this Objective must include at least one of the following entities: Operator of Essential Services (OES), as identified by the Member State in the context of with the NIS Directive; National or European Information Sharing and Analysis Centre (ISAC) having at least one OES as member; National Competent Authority (NCA) or Single Point of Contact (SPOC) designated by the Member States in line with the NIS Directive. Provided that these and related requirements are fulfilled, other sector associations can be part of the consortium as well.

23. Concerning Objective 1: Could the development of security requirements related to critical infrastructure security be considered as an eligible activity under this call?

Yes, provided that the requirements of the operator of essential services are for cybersecurity and that the proposal can justify their development under the terms of the objectives described in the call text and the Work Programme[4].

24. Concerning Objective 1: Can an OES in a sector that is not specified in Annex II of the NIS Directive apply?

Yes, provided that an OES has been identified or is in the process of being identified by the Member State as such, it can apply, in line with Section 6.1 of the call text. Please note that a letter of support, to be signed by the relevant Ministry/National Authority declaring that the applicant is or is in the process of being identified as an OES will have to be provided.

This reflects the following statement within the European Commission Communication *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union" (COM(2017)476)* (Section 4.1.3):

"Member States are in general free to expand the security and notification obligations under Article 14 to entities belonging to other sectors and sub-sectors than those listed in Annex II of the NIS Directive."

It is understood that this expansion will be undertaken in a transparent manner in tandem with the NIS Directive transposition process so that all relevant stakeholders, including the Commission, can be informed as to the identity and scope of the additional sectors and sub-sectors.

25. Concerning Objective 1: Will the costs of obtaining an ISO:27000 certification, and limited consultancy support to obtain the certification, be eligible in Actions of Objective 1?

Yes, provided that the certification serves the purpose of improving internal capabilities to meet security and reporting requirements under national and EU legislation, as stated in the call text. The resulting recommendations and guidelines could be shared with other OES through ISACs.The cost has be respect the provisions of article II.19.1 of the Grant Agreement in order to be considered as eligible.

[4] https://ec.europa.eu/inea/sites/inea/files/cef_telecom_work_programme_2019.pdf

26. Concerning Objective 1: An entity is not included in the national register of the Operators of Essential Services. Nevertheless, according to the Ministry responsible, the entity is providing an essential service and is thus an eligible applicant. Can the entity apply?

The enity can apply if it is an OES identified by the Member State in the context of with the NIS Directive. Accordingly, the entity can apply if it can submit with its proposal a Confirmation Letter for Operator of Essential Services (OES) applying to Objective 1, using the template available on the call webpage[5], which is signed by relevant Ministry/National Authority. This is the National Competent Authority that receives notifications from the applying OES, in accordance with Article 14 of the NIS Directive[6].

The template for relevant Ministry/National Authority requires the relevant Ministry or Authority to certify that the applicant is identified, or is in the process of being identified, as an OES in line with the NIS Directive.

If the entity does not meet the above described eligibility requirements, it could apply in consortium with an OES identified by the Member State in the context of with the NIS Directive depending on the types of activities that the proposal covers.

27. Concerning Objective 1: We are several entities part of the an economic group, which are identified by the National Competent Authority as Operators of Essential Services, in accordance with the NIS Directive. Is it possible to submit a joint application coordinated by the Group Holding (not identified as an OES) and having as beneficiaries, the remaining OES affiliated entities, or should each OES entity submit an application separately? In the case of a joint application, is it still necessary that the beneficiaries being affiliated entities of the Holding form a consortium?

As specified in section 6.1 of the call text, at least one applicant (i.e. not an entity affiliated to the applicant) has to be an OES identified by the Member State in the context of with the NIS Directive. It is possible to submit a joint application coordinated by the Group Holding only if at least one OES applies as partner. Depending on their status (please check the definition of affiliated entity in the General FAQ), the other OESs could be affiliated entities or additional partners.

The choice of forming a consortium or to submit separate applications (e.g. one per OES) depends on your own consideration on aspects such as the type of proposed activities and your organisational constraints.

28. Concerning Objective 1: Would a proposal submitted by an applicant which is not an OES and its affiliated entity which is an OES be eligible?

No. The section 6.1 of the call specifies that the Confirmation Letter must be submitted by Operators of Essential Services (OES) applying to call Objective 1. Therefore, the OES must be an applicant, not an affiliated entity.

29. Concerning Objective 1: The call requires that "Proposals involving existing or new ISACs should liaise with the Core Service Platform cooperation mechanism, the ISAC Facilities manager (SMART 2018/1022)". How can we find out more about this platform/mechanism in order to accurately address plans for liaison on both a technical and operational level?

Please refer to the document EU ISACs uploaded on the call page.

[5] Direct link to template: https://ec.europa.eu/inea/sites/inea/files/cefpub/2020-2_cybersecurity_obj_1_confirmation_letter_oes_final.doc

[6] Security of Network and Information Systems Directive (Directive (EU) 2016/1148)

30. Concerning Objective 1: Are there any other resources on the EU ISACs and how they should liaise with the Core Service Platform cooperation mechanism, the ISAC Facilities manager?

The information currently available to the public is referred to on the call page [here and here] and in these FAQs. Please note that the ISAC Facilities manager offers a series of services e.g. workshops, legal support and a technical platform. Therefore the liason is intended as interaction with these services. Concerning the technical platform, which is only a part of the services, it is currently being developed and technical details will be made available after the platform will have been developed.

31. Concerning Objective 1: We currently have a Security Information and Event Management system in place in the company. Would an upgrade of the system which leads to its automatisation be an eligible cost? Also, in case we decide to upgrade the current security infrastructure of the company (e.g., install new firewall), would the software updates and maintenance related to the firewall be an eligible cost within the period of the project? Moreover, would an upgrade of the log collection and anomaly detection system we have in place, which leads to its automatisation, be an eligible cost?

It depends on whether and how the proposed measures would fit in one of the objectives of the call. For example, under Objective 1 an Operator of Essential Services (OES), identified or in the process of being identified, in line with the NIS Directive, can apply for improving internal capabilities to meet security and reporting requirements under national and EU legislations. Accordingly, the proposal should clarify the addressed security and reporting requirements.

32. Concerning Objective 1, activity a): Would the involvement of two OES, one in position of "donor" of sectorial good practices in the field of Cybersecurity and the other in a "take-up" position, be possible?

Yes, provided that the types of activity specified under Objective 1 of the call are addressed.

33. Concerning Objective 1, activity a): Is it possible to apply for services that improve and increase security (firewalls, encryption of communication, prevention of interruptions)? Can we refer to a specific brand or upgrade from a Microsoft E3 licence to an E5?

Yes, it is possible to apply for such activities as long as they improve the organisation's internal capabilities in order to meet security and reporting requirements under national and EU legislation, as stated in the call. Please note that the proposals must clearly explain which security and reporting requirements will be addressed by the proposed activities.

Reference to specific brand or vendor in the proposal is possible. However, please note that the proposal should clearly explain how the referenced solution addresses the chosen call objective.

In order to be considered eligible, costs must espect the provisions of article II.19.1 of the Grant Agreement.

34. Concerning Objective 1, activity a): Is it possible to address cybersecurity aspects relating to IT systems for management of port/terminal operations?

Please refer to Q33 above.

35. Concerning Objective 1, activity a): Is the implementation of Security Information and Event Management (SIEM) solutions funded through CEF?

Please refer to Q31 and Q33 above.

36. Concerning Objective 1, activity a): Can a consortium of one OES and one DSP apply, taking into account that this DSP will provide all services for completion of all activities and the whole project?

The eligibility criteria for Objective 1 are specified under section 6.1 of the call text.

In a consortium of 1 OES and 1 DSP, the DSP could provide the services for the completion of all activities as long as it improves the OES's internal capabilities **in order to meet security and reporting requirements under national and EU legislation**, as stated in the call.

37. Concerning Objective 1, activity b): my organisation is an ISAC without legal personality. Can my organisation apply?

Proposals may be submitted by entities which do not have legal personality under the applicable national law, provided that their representatives have the capacity to undertake legal obligations on their behalf and offer a guarantee for the protection of the EU's financial interests equivalent to that offered by legal persons. If the ISAC does not have legal personality and does not meet the conditions described above, it is suggested that the ISAC members apply as a consortium, provided that the eligibility requirements of the call (e.g. at least one applicant must be a OES) are respected.

38. Concerning Objective 1, activity b): the call text states that "ISACs, already existing or to-be set up, should be chaired by an OES". What does it mean exactly?
Also, is it recommended that the OES acts as the project's coordinator?

The ISAC should be chaired by an Operator of Essential Services (OES) so that it is reflective of the interests of the OES categories. It is essential that the work of the ISAC is being steered and controlled by OES.

In line with the call text, it is not required that an OES is the coordinator of the Action.

39. Concerning Objective 1, activity b): Until when should the OES chair of the ISAC last?

The ISAC should be chaired by an Operator of Essential Service (OES) for the duration of the Action. In section 3 of the application form part D, applicants must address the *Impact and Sustainability* award criterion, as well as its sub-criteria. The long-term sustainability of the created ISAC must be addressed in this section.

Please also see section 4.5 of the Guide for Applicants.

40. Concerning Objective 1: What exactly is an Operator of Essential services (OES)? How is it possible to identify the OES, the ISAC and the NCA at national level?

Operators of Essential services are identified by the Member State in the context of the NIS Directive (the Directive (EU) 2016/1148 on Security of Network and Information Systems). The NIS Directive establishes the following criteria for the identification of the operators of essential services by Member States under article 5.2: (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.

The National Competent Authority (NCA) or Single Point of Contact (SPOC) are designated by the Member States in line with the NIS Directive. An overview of NCAs/SPOCs per Member State is available here: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

For the purposes of this call, a national or European ISAC is defined as a legal entity that is a trusted entity fostering information sharing and good practices about physical and cyber threats and mitigation among its members. European ISACs are defined as ISACs with members coming from different Member States, while National ISACs are defined as ISACs where the members are coming from one Member State. More information about ISACs is available on ENISA's website: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

41. Concerning Objective 1: The recognition as OES by the Ministry is enough to prove the national recommendation?

In order to be eligible under objective 1, OESs must download from the call webpage[7], fill in, and upload as a supporting document, the Confirmation letter, to be signed by the relevant Ministry/National Authority - declaring that the entity is identified or is in the process of being identified as an OES. This requirement must be fulfilled within the specified timeline, otherwise the Agency reserves the right to cancel the grant agreement preparation.

42. Concerning Objective 1: Are both public and private port operators eligible to apply if they have the approval of the competent MS authority?

Public and private port operators can apply as OES if the above mentioned confirmation letter is provided. If they do not comply with any of the eligibility requirements indicated in section 6.1 of the call, they could apply as partners in a consortium with other entities that do meet those requirements.

43. Concerning Objective 1: Can we use the same Confirmation letter for OES submitted for the 2019 call or do we have to ask the relevant Ministry to issue it again?

The Confirmation Letter for the 2020 call is the only document accepted to prove the OES status of applicants. Previous confirmation letters will not be accepted.

Please note that the Confirmation Letter is a requirement in addition to the Member State approval (Form A 2.3).

44. Concerning Objective 2: Could you please provide examples of "national public authorities..." and "legal entities entrusted..." as decribed under Objective 2?

Examples of the categories described above would be National Competent Authorities; Single Points of Contacts; National CSIRTs as designated/identified in line with the NIS Directive. These should be entities relevant for the implementation of the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (the "Cyber Blueprint") and the Commission proposal for a Joint Cyber Unit.

45. Concerning Objectives 1 and 2: Is it possible that several countries could address objective 1 or 2 (or both) as partners?

Yes, applicants from several countries could address Objectives 1 or 2 (or both) as partners, provided that the consortium meets the eligibility requirements outlined in section 6.1 of the call text. The countries of the applicants can be neighbouring countries or non-neighbouring countries.
Please be reminded that proposals may address only ONE objective and the eligibility requirements for each call objective are outlined under section 6.1 of the call text. Do note that additional requirements apply to third countries and third countries applicants (i.e. not from EU Member States or EEA countries).

[7] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

46. <u>Concerning Objectives 1 and 2:</u> How many Member States should participate under objective 1 and objective 2 of the call? Is there a minimum number or not?

Proposals under Objectives 1 and 2 can be submitted either by a single applicant or by a consortium of applicants from a single country or several countries.

Such a consortium does not have a minimum or maximum number of partners or Member States. However, for Objective 2, while proposals from a single entity are eligible, the call also states that proposals including cross-border cooperation activities for effective joint cybersecurity operations and/or building mutual trust are particularly encouraged.

47. <u>Concerning Objectives 1 and 2</u>: Is a local authority, such as a borough recognised as an OES, eligible under Objectives 1 and 2?

Yes, if it complies with the eligibility requirements outlined under section 6.1 of the call text. A local authority, that is an Operator of Essential Services (OES) as identified by the Member State in the context of the NIS Directive, may apply as a single applicant or as a member of a consortium under Objective 1. Generally, even if an organisation, e.g. a local authority, does not comply with any of the eligibility requirements indicated in section 6.1 of the call, it could still apply as a partner in a consortium with other entities that do meet those requirements. For example, proposals submitted under Objective 2 must include at least one of the following entities: national public authorities, national public bodies or a legal entity entrusted with national level cybersecurity. A local authority would normally not fall under these categories, but it could be part of a consortium with such entities.

48. <u>Concerning Objective 4:</u> One of the requirements under this Objective is that the applicant must be a NCCA (National Cybersecurity Certification Authority) /NAB (National Accreditation Body)/CAB (Conformity Assessment Body) in order to be eligible. Does the CAB need to be dedicated only to cybersecurity, or can it be a more general entity with a division/department that works on cybersecurity?

In order to be eligible, a CAB should be an entity accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. If accredited, either type of CAB i.e. those dedicated solely to cybersecurity or those with designated cybersecurity departments would be eligible under this call.

In other words, generalist CABs – for example carrying out conformity assessment in a wide range of sectors (safety, security etc) and specialised CABs - for example carrying out conformity assessment in ICT security – may apply, as long as they are accredited according to Regulation (EC) No 765/2008. We therefore strongly encourage applicants to pay careful attention to the provisions of this Regulation, pursuant to which a CAB is to be appointed and defined as an entity accredited by national accreditation bodies. Please also keep in mind that the recipient of funds must be located in a EU/EEA Member State.

As part of the application to this call, each CAB must complete and upload (as a supporting document) the self-declaration form confirming that the entity is a CAB. The form is available on the call webpage: https://ec.europa.eu/inea/sites/inea/files/cefpub/2020-2_cybersecurity_obj_4_self-declaration_final.doc.

If the proposal is retained for funding, the applicant will have to demonstrate its status of accredited CAB before the signature of the grant agreement.

Generally, even if a CAB does not comply with any of the eligibility requirements indicated in section 6.1 of the call, it could still apply as a partner in a consortium with other entities that do meet those requirements.

49. We see that the template of the confirmation letter for OES was updated 23 October. What changes have been implemented?

The previous version of the letter referred to OESs only as "applicants". However, an OES mentioned in the self-declaration of an applying ISAC must provide the OES confirmation letter, even if the said OES is not an applicant. The confirmation letter has been corrected to take into account both cases. See also Q50 below.

50. We already have a signed version of the confirmation letter for OES on the previous template. Do we also need to provide a version on the updated template?

No. Confirmation letters for OES on both (old and new) versions of the template will be accepted.

The following questions raised during the webinar "Learn about EU funding opportunity on capacity building for cybersecurity certification" held on 13/10/2020: https://ec.europa.eu/digital-single-market/en/news/learn-about-eu-funding-opportunity-capacity-building-cybersecurity-certification

General questions:

W1. What is the co-financing rate?

As indicated in section 11.1 of the call text, the maximum co-financing rate is 75% to the eligible costs. Such costs are:

(a) actually incurred and declared by the beneficiary and its affiliated entities.
(b) a flat rate of 7 % of the eligible direct costs ('reimbursement of flat-rate costs')

W2. What should the duration of a project be?

As indicated in section 6.2 of the call text, the indicative duration of an Action is 36 months. Note that this duration is not mandatory. However the duration should be coherent with the proposed activities.

Questions specific to Objective 4:

W3. Concerning Objective 4: What types of organisations are eligible under this objective? Are industries 'using' certifications or contributing to evaluations/certification standards eligible to participate in this call?

With the agreement of the Member State(s) or EEA countr(y)ies concerned (form A 2.3 of the application form), international organisations, Joint Undertakings, or public or private undertakings or bodies can apply to this call. Section 6.1 of the call text indicates specific additional eligibility requirements for each objective. For objective 4, proposals submitted must include at least one of the following entities:

- **National Cybersecurity Certification Authority (NCCA), officially designated, or in the process of being designated**, by a Member State in line with the Cybersecurity Act.
  N.B: Each NCCA in the process of being designated as such must download from the call webpage, fill in, and upload as a supporting document the Confirmation Letter, to be signed by the competent Ministry/National Authority declaring that the applicant is in the process of being identified as an NCCA.

- **National Accreditation Body located in an EU Member State appointed pursuant Regulation (EC) No 765/2008**.

- **Conformity Assessment Body (CAB) defined as an entity accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008**.

N.B: Each CAB must download from the call webpage, fill in, and upload as a supporting document the self-declaration confirming that the entity is a CAB.

If an entity does not meet these additional eligibility requirements, it could apply as partner in a consortium with other entities that do meet those requirements. Please note that the activities proposed must be relevant to the call.

W4. Concerning Objective 4: The National Cybersecurity Certification Authority (NCCA) of my country is in the process of being designated as such. Can it apply as NCCA under objective 4?

Yes, as specified in Section 6.1 of the call text, a National Cybersecurity Certification Authority (NCCA) either officially designated, or in the process of being designated, by a Member State in line with the Cybersecurity Act is eligible under objective 4. Each NCCA in the process of being designated as such must complete the Confirmation Letter and upload as a supporting document with the application. The letter must be signed by the competent Ministry/National Authority declaring that the applicant is in the process of being identified as an NCCA. (The competent Ministry/National Authority is the entity responsible for the designation of the national cybersecurity certification authority in accordance with Article 58(1) of the Cybersecurity Act.). Please also note that changes to the template of the Confirmation Letter might lead to the ineligibility of the applicant.

If the proposal is retained for funding, entities in the process of being designated as NCCAs at the moment of submission will have to demonstrate their NCCA status before the signature of the grant agreement (see the indicative timing for preparation and signature of grant agreements under section 3 of the call text). This requirement must be fulfilled within the specified timeline; otherwise INEA reserves the right to cancel the grant agreement preparation.

W5. Concerning Objective 4: In case EU cybersecurity certification schemes under the framework are not yet available, could a CAB still participate even if it cannot become accredited in the context of European cybersecurity certification schemes?

Does the applying CAB need to have existing cybersecurity scope?

An entity in a Member State is currently preparing an application for objective 4 in its capacity as a prospective conformity assessment body for cybersecurity certification schemes under the EU Cyber Security Act. This entity is a public body and is presently accredited as a conformity assessment body by the national accreditation authority for ISO 27000 (Information Security Management System). However the entity is not accredited as a conformity assessment body under the EU Cyber Security Act. Would it still be eligible to participate in this call?

For objective 4, proposals submitted must include at least one NCCA or one National Accreditation Body or one CAB (Conformity Assessment Body). A CAB is defined as an entity accredited by National Accreditation Bodies appointed pursuant to Regulation (EC) No 765/2008.

There is no specific eligibility requirement to be an accredited CAB in the context of EU cybersecurity certification schemes as they are not there yet.

In other words, a CAB (generalist or specialised) is eligible under Objective 4 as long as it is accredited according to Regulation (EC) No 765/2008. As an alternative way of participation, a CAB that is not accredited according to this Regulation, could still apply as a partner in a consortium with other entities that do meet the eligibility requirement set out in the section 6.1 of the call text.

W6. Concerning Objective 4: Does our proposal have to involve more than one CAB or can it be presented by just one CAB?

It can be submitted by just one CAB because there is no obligation to form a consortium under objective 4.

W7. <u>Concerning Objective 4</u>: Does Objective 4 imply that at least two Member States have to cooperate?

There is no consortium requirement for Objective 4, although this does not prevent Member States from teaming up. They are encouraged to do so under activity b) *cross-border exchange of good practices and relevant information related to conformity assessment activities, and peer support on technical issues related to carrying out cybersecurity audits of conformity assessment bodies*.

W8. <u>Concerning Objective 4</u>: Are the activities under this objective (a/b/c) listed by priority?

No, activities (a/b/c) are not listed by priority;. Proposals should address at least one of the activities, without order of preference.

W9. <u>Concerning Objective 4</u>: Is there any limit for number of eligible applicants?

No. The size and profile of a consortium should be in line with the needs of the proposal's tasks and objectives, among others, the quality and relevant experience of the participants will be assessed in the proposal evaluation.

W10. <u>Concerning Objective 4:</u> What budget is envisaged to be awarded to individual projects?

Out of the total call budget of €10.5 million, €1 million is earmarked under Objective 4. The earmarked budget refers to the whole of the objective and it is not intended as a funding ceiling for single proposals, i.e. there is no funding ceiling per proposal. In any case, the budget requested should be coherent with the proposed activities.

W11. <u>Concerning Objective 4:</u> Which projects on cybersecurity certification have been awarded in the past?

Please see the following links to the relevant project descriptions:

1. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-eu-ia-0109
2. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-sk-ia-0073
3. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-be-ia-0117

W12. <u>Concerning Objective 4:</u> We'd like to gather NCCA, CABs and industry representatives to work on a cybersecurity evaluation methodology and catalogue of attacks for future schemes. From our understanding, the project leader would be entitled to managed the funds and provide the related proofs to the Commission. In the case of a consortium made of NCCA, CABs and industry and private actors, could a private entity (other than a NCCA or a CAB) be the project leader?

There is no requirement or preference concerning the applicant who can be the coordinating applicant in a multi-applicant proposal, provided such applicant meets the eligibility and selection criteria specified in the call text. In the case described, a private entity other than a NCCA or a CAB can be the coordinator.

Please see article II.1.3 of the model grant agreement for the general obligations and role of the project coordinator.