EUROPEAN COMMISSION
INNOVATION AND NETWORKS EXECUTIVE AGENCY

CALL FOR PROPOSALS CONCERNING PROJECTS OF COMMON INTEREST UNDER THE CONNECTING EUROPE FACILITY IN THE FIELD OF TRANS-EUROPEAN TELECOMMUNICATION NETWORKS

CEF TELECOM CALLS 2020

CEF-TC-2020-2: Cybersecurity

1. BACKGROUND AND RATIONALE

The general context for this call for proposals is defined in section 3.9 of the 2019-2020 Connecting Europe Facility (CEF) Telecom Work Programme[1] as published on the call page on the Innovation and Networks Executive Agency (INEA) website.[2] The background and rationale for this call for proposals are defined in section 3.9.1 of the 2019-2020 Work Programme.

2. PRIORITIES & OBJECTIVES

2.1 Priority outcomes

The priorities of this call for proposals are defined in section 3.9.2.2 of the 2019-2020 Work Programme.

Applicants who already received CEF funding under previous CEF Telecom Cybersecurity calls and who plan to apply again under this call must clearly explain in section 1 and 2.1 of the application form part D of their proposal how their proposed Action will build on and/or differ from the Action(s) funded under the previous call(s).

The Objectives of this call and the activities that could be funded are described below.

Under this call, proposals will be funded that address only one of the objectives listed below. Applicants must clearly indicate in the proposal summary and application

[1] Commission Implementing Decision C(2020)1078 of 28 February 2020 amending a Multi-Annual Work Programme 2019 and 2020 for financial assistance in the field of Connecting Europe Facility (CEF) Telecommunications sector
[2] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

form part D of their proposal which of the following objectives their proposal adresses.

Objective 1: Support for Operators of Essential Services (OES), National Competent Authorities, and Information Sharing and Analysis Centres (ISACs).

Under the Directive (EU) 2016/1148 on Security of Network and Information Systems (the "NIS Directive" [3]), identified Operators of Essential Services (OES) have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority i.e. National Competent Authorities (NCAs)/Single Points of Contact (SPOCs).

The aim of this objective is to facilitate the creation of a coherent ecosystem for risk management, information sharing and reporting in Member States, by helping relevant stakeholders to comply with the NIS Directive and supporting the interaction between the public and the private sector, including through Information Sharing and Analysis Centres (ISACs).

Proposals submitted under this Objective **must** include **at least one** of the following entities:

- **Operator of Essential Services (OES)**, as identified, or in the process of being identified, in line 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)**, as designated in line with the NIS Directive.

Proposals should address **at least one** of the activities outlined below.

a) **OES(s) improving internal capabilities to meet security and reporting requirements under national and EU legislation**. Examples include risk assessments, penetration testing and audits to get a better grasp on security maturity levels, exercises, and internal training. Proposals must clearly explain which security and reporting requirements will be addressed by the proposed activities, and should take the guidance documentation published by the NIS Cooperation Group into account[4].

   The application should clearly explain which services are addressed and how.

b) **OESs and/or ISACs setting-up a new/improving an existing national or European level ISAC** to enhance the cybersecurity preparedness of OESs through effective information sharing and improved situational awareness.

   ISACs, already existing or to-be set up, should be chaired by an OES, and should be representative of industry stakeholders. They should also involve, or otherwise

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[4] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

clarify their link with public authorities. Furthermore, the call encourages applications concerning ISACs that cover a sector or subsector as set out in Annex II of the NIS Directive or are identified as relevant in its national transpositions. Relevant documentation made available by the European Union Agency for Network and Information Security (ENISA)[5] should be taken into account in this regard.

c) **NCAs/SPOCs supporting the national ISAC ecosystem or its development** with technical and logistical activities. This could include e.g. the organisation of meetings for ISAC members, providing support to ISAC's management, hosting an IT platform to exchange information, centralising analysis capabilities for by all ISACs in the country, etc.

Proposals including more than one type of entities (e.g. a consortium of a NCA and an OES) should choose the most appropriate activity/activities (a, b, c) among those listed above.

All proposals should demonstrate the successful impact of the proposed activities at the end of the Action.

Proposals involving existing or new ISACs should liaise with the Core Service Platform cooperation mechanism, the ISAC Facilities manager (SMART 2018/1022). Where relevant, beneficiaries funded under this Objective should participate in events and other activities organised by the ISAC Facilities manager and/or use its support services and/or join a relevant ISAC.

[5] Publications by ENISA on this topic are available here: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Objective 2: Support to joint preparedness, shared situational awareness and coordinated response to cybersecurity incidents

In line with the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (the "Cyber Blueprint")[6] and the Commission proposal for a Joint Cyber Unit, this objective supports cooperation for joint preparedness and shared situational awareness about cyber threats at the Member State and EU level, as well as coordinated response and mutual assistance in times of crisis.

Proposals submitted under this Objective **must** include **at least one** of the following entities:

- National public authorities and national public bodies
- Legal entities entrusted with national level cybersecurity

Proposals including cross-border cooperation activities for effective joint cybersecurity operations and/or building mutual trust are particularly encouraged. Co-operation activities should facilitate the continuation or creation of stable cross-border relationships.

Proposals should address **at least one** of the activities below:

a) **developing and deploying cyber range platforms and strategic and/or operational Cyber Threat intelligence (CTI) frameworks, programs and/or tools**. These should aim at preparing the participating entities to defend high-risk, critical cyber systems and organisations against advanced, known and new cyberattacks, and to reduce their security risks. Proposed actions funded under this Objective should foresee participation in coordination activities and events organised by relevant European cybersecurity Institutions (e.g. ENISA, CERT-EU). Proposals should demonstrate knowledge, and as appropriate build upon, relevant results from research and innovation in this area, in particular from actions funded by the Horizon 2020 Programme.

b) **designing, developing and delivering structured trainings**, including cybersecurity exercises, to prepare cyber defenders in both public and private organisations to protect their critical infrastructures. Proposed actions funded under this Objective should foresee participation in coordination activities and events organised by relevant European cybersecurity Institutions (e.g. ENISA, CERT-EU).

c) **further developing and implementing the European Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises,** and the Commission proposal on a "Joint Cyber Unit", in particular through secure and resilient governmental communication mechanisms, rapid response mechanisms, hybrid threat monitoring, mutual assistance initiatives and related cyber or hybrid exercises. Beneficiaries will be expected to consider the use of the Standard Operating Procedures developed by the European Union institutions and Member States on the basis of the Recommendation.

[6] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises: https://eur-lex.europa.eu/eli/reco/2017/1584/oj

All proposals should demonstrate the successful impact of the proposed activities at the end of the Action.

Objective 3: Support to the implementation of cooperation activities of the Second Biannual Work Programme of the NIS Cooperation Group (2020-2022)

This objective supports cross-border cooperation aiming at strengthening the know-how and capabilities of the national public authorities and bodies participating in the NIS Cooperation group, which is being set-up by the NIS Directive.

Proposals submitted under this Objective **must** include national public authorities and/or national public bodies from **at least two different Member States**.

Proposals should address activities developing and implementing cooperation activities in line with the Second Biennial Work Programme of the Cooperation Group (2020-2022).

These activities should aim to create mutual trust and confidence and facilitate knowledge sharing, as well as build effective joint working methods and increase national capacities in the cybersecurity domain.

Examples include:

- staff exchanges between NCAs/SPOCs lasting several weeks, allowing participants to familiarise themselves with the work of the hosting country in the field of cybersecurity, for example through job shadowing, study visits or cooperation meetings. These exchanges should be aimed at facilitating cooperation and increasing the professional skills of individual members of the respective cybersecurity teams;
- voluntary evaluation of national frameworks (peer reviews).

Proposals for staff exchanges are highly encouraged.

All proposals should demonstrate the successful impact of the proposed activities at the end of the Action.

The amount of funding expected to be allocated under this objective is €1 million out of the total budget for the call of €10.5 million.

Objective 4: Support to cooperation and capacity building for cybersecurity certification in line with the Cybersecurity Act

Funding will be granted to improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 ("Cybersecurity Act")[7].
Proposals submitted under this objective **must** include **at least one** of the following entities:

- **National Cybersecurity Certification Authority**, officially designated, or in the process of being designated, by a Member State in line with the Cybersecurity Act
- **National Accreditation Body** located in an EU Member State appointed pursuant Regulation (EC) No 765/2008
- **Conformity Assessment Body**, defined as an entity accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008.

Proposals should address **at least one** of the activities outlined below:

a) **building up or enhancing internal capabilities** to effectively undertake conformity assessment activities, as set out in the Cybersecurity Act. For example proposals may include upskilling staff and training (e.g. on how to use testing equipment, run cybersecurity audits, write protection profiles, certification reports) or acquisition and use of relevant equipment and infrastructure (e.g. equipment to test IT systems such as pen-testing, IT support to facilitate documentation review).
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. Activities may range from staff exchanges, development of good practice databases. Funding for these activities aims to promote synergies and mutual recognition of the results of conformity assessment activities across Member States.
   Proposed cross-border exchanges should include National Cybersecurity Certification Authorities, designated or in the process of being designated, from at least two different Member States.
c) **development and implementation of efficient evaluation methods** that can bring tangible benefits e.g. shorter duration of the certification process. These evaluation methods may be applicable for the evaluation of ICT products, services and processes used in one or more specific sectors.

Where relevant, beneficiaries funded under this Objective should contribute to activities organised in the context of European cooperation platform for cybersecurity certification which is being set-up by the European Commission and is expected to be launched in 2021. In addition, National Cybersecurity Certification Authorities, and public entities that have primary responsibility for cybersecurity certification at national level should participate in working groups of the European Cybersecurity Certification Group established in line with the Cybersecurity Act.

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act): https://eur-lex.europa.eu/eli/reg/2019/881/oj

The amount of funding expected to be allocated under this objective is €1 million out of the total budget for the call of 10.5 million.

2.2 Results expected from the financial assistance

The benefits and expected outcomes of this call for proposals are defined in section 3.9.2.3 of the 2019-2020 Work Programme.

The call will assist the Member States to improve cybersecurity resilience in general and limit the economic and political damage of cyber incidents, while reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.

The call aims to improve compliance with the NIS Directive and the Cybersecurity Act.It supports the implementation of Commission Recommendations on cybersecurity as well as promoting higher levels of situational awareness and crisis response in Member States. This will open new avenues for cross European cooperation in cybersecurity, stimulating convergence of approaches and behaviour, and leading to higher preparedness and better cybersecurity resilience.

3. TIMETABLE

Date of publication of call for proposals	Tuesday 30 June 2020
Deadline for the submission of proposals	Thursday 5 November 2020 (17:00.00 Brussels time)
Evaluation of proposals	November 2020 – January 2021 (indicative)
Consultation of the CEF Committee	March – April 2021 (indicative)
Adoption of the Selection Decision	April 2021 (indicative)
Preparation and signature of grant agreements	Between May and August 2021 (indicative)

4. BUDGET AVAILABLE

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.

The Commission reserves the right not to distribute all the funds available.

The Commission reserves the right to award a grant of less than the amount requested by the applicant.

5. ADMISSIBILITY REQUIREMENTS

In order to be admissible, proposals must be:

- Submitted electronically in the TENtec Information System eSubmission module.[8] In this respect, proposals or part(s) of proposals submitted by email or in hard copy shall not be admissible.
- Submitted by the deadline for submission of proposals (see sections 3. "Timetable" and 14.2."Submission process").
- Complete (i.e. application forms (A, B, C and D) are uploaded in the TENtec eSubmission module).
- Duly signed by the applicant(s).

Failure to comply with any of these requirements will lead to the rejection of the application.

6. ELIGIBILITY CRITERIA

6.1 Eligible applicants

In accordance with the 2019–2020 Work Programme and pursuant to Article 9 of the CEF Regulation,[9] only those proposals submitted by the following types of applicants are eligible:

- One or more Member State(s);
- With the agreement of the Member State(s) or EEA countr(y)ies concerned, international organisations, Joint Undertakings,[10] or public or private undertakings or bodies established in Member States.

Additional requirements

For Objective 1:

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.

[8] The TENtec eSubmission module is part of the TENtec Information System used to manage CEF actions during their entire lifecycle and enables the electronic submission of proposals under the CEF calls. The link to TENtec is available under the "Application Forms" section of the call webpage: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

[9] Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 Text with EEA relevance, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1316

[10] For the purposes of this call, a Joint Undertaking means a joint undertaking established by the EU for the efficient execution of EU research, technological development and demonstration programmes, as referred to in Article 187 of the Treaty on the Functioning of the European Union, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Each OES must download from the call webpage[11], fill in, and upload as a supporting document the Confirmation letter, 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. Where the same Ministry/National Authority is responsible for the identification of several applicants as OESs, it is possible to submit one Confirmation letter listing all the relevant applicants. If their proposal is retained for funding, entities in the process of being identified as OESs at the moment of submission will have to demonstrate their OES status before the signature of the grant agreement (see the indicative timing for preparation and signature of grant agreements under section 3). This requirement must be fulfilled within the specified timeline; otherwise the Agency reserves the right to cancel the grant agreement preparation.

Changes to the text of the "Template for the Confirmation Letter" might lead to the ineligibility of the applicant.

- **National or European Information Sharing and Analysis Centre (ISAC)** having at least one OES as member.

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 most members are coming from one Member State.

The ISAC must download from the call webpage[12], fill in, and upload as a supporting document the self-declaration, confirming that the entity is a national or European ISAC and that at least one OES is a member.

The Operator of Essential Services (OES) must be identified by the Member State in the context of the NIS Directive. All OESs must download from the call webpage[13], 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 or is in the process of being identified as an OES. Where the same Ministry/National Authority is responsible for the identification of several OESs, it is possible to submit one letter of support listing all relevant entities. If the proposal is retained for funding, entities in the process of being identified as OESs at the moment of submission will have to demonstrate their OES status before the signature of the grant agreement (see the indicative timing for preparation and signature of grant agreements under section 3). This requirement must be fulfilled within the specified timeline; otherwise the Agency reserves the right to cancel the grant agreement preparation.

Changes to the text of the "Template for the Self-Declaration" might lead to the ineligibility of the applicant.

- **National Competent Authority (NCA) or Single Point of Contact (SPOC)** designated by the Member States in line with the NIS Directive.

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

For Objective 2:

Proposals submitted under this Objective **must** include **at least one** of the following entities:
- National public authorities and national public bodies
- Legal entities entrusted with national level cybersecurity.

For Objective 3:

Proposals submitted under this Objective **must** include national public authorities and/or national public bodies from **at least two different Member States**.

For Objective 4:

Proposals submitted under this objective 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.
Each NCCA in the process of being designated as such must download from the call webpage[14], 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. 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. 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). This requirement must be fulfilled within the specified timeline; otherwise the Agency reserves the right to cancel the grant agreement preparation. Changes to the text of the "Template for the Confirmation Letter" might lead to the ineligibility of the applicant.

- **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. Each CAB must download from the call webpage[15], fill in, and upload as a supporting document the self-declaration confirming that the entity is a CAB. 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 (see the indicative timing for preparation and signature of grant agreements under section 3). This requirement must be fulfilled within the specified timeline; otherwise the Agency reserves the right to cancel the grant agreement preparation.

Changes to the text of the "Template for the Self-Declaration" might lead to the ineligibility of the applicant.

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

EEA countries
In accordance with section 5.3.1 of the 2019–2020 Work Programme, European Free Trade Association (EFTA) countries which are members of the European Economic Area (EEA) may participate[16] in the call for proposals, even when not explicitly mentioned in the Work Programme text, with the same rights, obligations and requirements as EU Member States. At the time of call publication, these conditions apply to Norway and Iceland only.[17]

For UK applicants: Please be aware that following the entry into force of the EU-UK Withdrawal Agreement[18] on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to natural or legal persons residing or established in a Member State of the European Union are to be understood as including natural or legal persons residing or established in the United Kingdom. UK applicants are therefore eligible to participate under this call.

Third countries and third country entities
Where necessary to achieve the objectives of a given project of common interest and where duly motivated, third countries and entities established in third countries may participate in actions contributing to the projects of common interest. They may not receive funding under the CEF Regulation, except where it is indispensable to achieve the objectives of a given project of common interest.

Acceding states and candidate countries benefiting from a pre-accession strategy may also participate in the sector of the CEF covering telecommunications infrastructure in accordance with agreements signed with the EU. As at the time of call publication no such agreements have been signed, the same conditions as for third countries apply to acceding states and candidate countries.

Third countries and entities established in third countries may only participate as part of a consortium with applicants from EU/EEA countries. The application must contain the agreement of the Member State concerned by the proposed Action and a declaration from the European partner involved in the proposal on why the participation of the third country applicant is indispensable. Applicants that are entities established in a third country must also provide proof of the support of the third country authorities concerned by the action.

Applicants without legal personality
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.

Natural persons
Proposals submitted by natural persons are not eligible.

Affiliated entities

[16] According to article 7.2 of Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructures and repealing Decision No 1336/97/EC.
[17] For the purposes of this call, Liechtenstein is considered a third country.
[18] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.

Applicants may designate affiliated entities within the meaning of Article 187 of the Financial Regulation[19], for the purpose of supporting the implementation of the action submitted for funding. Such affiliated entities must comply with the eligibility criteria for applicants.

Member State agreement
Any applicant that cannot provide the agreement of the EU Member State or EEA country concerned will not be eligible.

6.2 Eligible actions

In line with Article 7 of the CEF Regulation, only actions contributing to "projects of common interest" as identified in the Telecom Guidelines[20] shall be eligible for support through EU financial aid in the form of grants.

Please note that failure to comply with any of the eligibility criteria indicated above will lead to the rejection of the application.

Implementation period

The Action may not start before the date of submission of the application.[21]

Indicative duration

The indicative duration of an Action proposed under this call is 36 months.

7 EXCLUSION CRITERIA

7.1 Exclusion

An applicant shall be excluded from participating in call for proposals procedures where:

(a) the applicant is bankrupt, subject to insolvency or winding-up procedures, where its assets are being administered by a liquidator or by a court, where it is in an arrangement with creditors, where its business activities are suspended, or where it is in any analogous situation arising from a similar procedure provided for under national laws or regulations;
(b) it has been established by a final judgment or a final administrative decision that the applicant is in breach of its obligations relating to the payment of taxes or social security contributions in accordance with the applicable law;
(c) it has been established by a final judgment or a final administrative decision that the applicant is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the applicant

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1046
[20] Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC (Text with EEA relevance) See specifically Article 4 and the Annex for more information. See http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014R0283
[21] The date when the proposal was last submitted in the TENtec eSubmission module will be considered as the submission date of the proposal.

belongs, or by having engaged in any wrongful intent or gross negligence, including, in particular, any of the following:

(i) fraudulently or negligently misrepresenting information required for the verification of the absence of grounds for exclusion or the fulfilment of eligibility or selection criteria or in the performance of a contract, a grant agreement or a grant decision;

(ii) entering into agreement with other applicants with the aim of distorting competition;

(iii) violating intellectual property rights;

(iv) attempting to influence the decision-making process of the Commission/Agency during the award procedure;

(v) attempting to obtain confidential information that may confer upon it undue advantages in the award procedure;

(d) it has been established by a final judgment that the applicant is guilty of any of the following:

(i) fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 of the European Parliament and of the Council and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995;

(ii) corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 or Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997, or conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA, or corruption as defined in the applicable law;

(iii) conduct related to a criminal organisation, as referred to in Article 2 of Council Framework Decision 2008/841/JHA;

(iv) money laundering or terrorist financing, within the meaning of Article 1(3), (4) and (5) of Directive (EU) 2015/849 of the European Parliament and of the Council;

(v) terrorist offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA, respectively, or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 4 of that Decision;

(vi) child labour or other offences concerning trafficking in human beings as referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council;

(e) the applicant has shown significant deficiencies in complying with main obligations in the performance of a contract, a grant agreement or a grant decision financed by the Union's budget, which has led to its early termination or to the application of liquidated damages or other contractual penalties, or which has been discovered following checks, audits or investigations by an authorising officer, OLAF or the Court of Auditors;

(f) it has been established by a final judgment or final administrative decision that the applicant has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95;

(g) it has been established by a final judgement or final administrative decision that the applicant has created an entity in a different jurisdiction with the intent to circumvent fiscal, social or any other legal obligations of mandatory application in the jurisdiction of its registered office, central administration or principal place of business;

(h) it has been established by a final judgement or final administrative decision that an entity has been created with the intent referred to in point (g);
(i) for the situations referred to in points (c) to (h) above, the applicant is subject to:
    (i) facts established in the context of audits or investigations carried out by European Public Prosecutor's Office after its establishment, the Court of Auditors, the European Anti-Fraud Office or the internal auditor, or any other check, audit or control performed under the responsibility of an authorising officer of an EU institution, of a European office or of an EU agency or body;
    (ii) non-final judgments or non-final administrative decisions which may include disciplinary measures taken by the competent supervisory body responsible for the verification of the application of standards of professional ethics;
    (iii) facts referred to in decisions of persons or entities being entrusted with EU budget implementation tasks;
    (iv) information transmitted by Member States implementing Union funds;
    (v) decisions of the Commission relating to the infringement of the Union's competition law or of a national competent authority relating to the infringement of Union or national competition law; or
    (vi) decisions of exclusion by an authorising officer of an EU institution, of a European office or of an EU agency or body.

7.2 Remedial measures

If an applicant/affiliated entity declares one of the situations of exclusion listed above (see section 7.1), it must indicate the measures it has taken to remedy the exclusion situation, thus demonstrating its reliability. This may include e.g. technical, organisational and personnel measures to correct the conduct and prevent further occurrence, compensation of damage or payment of fines or of any taxes or social security contributions. The relevant documentary evidence which illustrates the remedial measures taken must be provided in annex to the declaration. This does not apply for situations referred in point (d) of section 7.1.

7.3 Rejection from the call for proposals

The authorising officer shall not award a grant to an applicant who:
(a) is in an exclusion situation established in accordance with section 7.1; or
(b) has misrepresented the information required as a condition for participating in the procedure or has failed to supply that information; or
(c) was previously involved in the preparation of documents used in the award procedure where this entails a breach of the principle of equal treatment, including distortion of competition, that cannot be remedied otherwise.

The same exclusion criteria apply to affiliated entities. Applicants and their affiliated entities, if applicable, must certify that they are not in one of the situations listed above.

Administrative sanctions (exclusion) may be imposed on applicants, or affiliated entities where applicable, if any of the declarations or information provided as a condition for participating in this procedure prove to be false.

7.4 Supporting documents

Applicants and affiliated entities must provide a declaration on their honour certifying that they are not in one of the situations referred to in Articles 136(1) and 141 of the Financial Regulation, by filling in application form Part B1 (for applicants) or B2 (for affiliated entities) accompanying the call for proposals and available at under the "Application Forms" section of the call webpage: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity.

8. SELECTION CRITERIA

The selection criteria are referred to in Annex 2 of the Work Programme. The financial and operational capacity of applicants and designated affiliated entities will be assessed as specified below.

The requirement to demonstrate financial and operational capacity also applies to designated affiliated entities **only where,** according to the proposal, the affiliated entity(ies) will be the only one(s) implementing the proposed Action.

Exceptions: The requirement for applicants to demonstrate their financial and operational capacity **does not** apply to Member States, public sector undertakings or bodies established in the EU/EEA countries (Norway and Iceland), third countries, international organisations, European Economic Interest Groupings (EEIG)[22] in which at least one member is a public sector body, Joint Undertakings, and transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC and certified following the procedures laid down in Articles 10 or 11 of Directive 2009/72/EC[23] or Articles 10 or 11 of Directive 2009/73/EC[24].

Applicants should register in the Participant Register and provide a Participant Identification Code (PIC, 9-digit number), serving as the unique identifier of their organisation. More information is available in the guidance on "Rules on Legal Entity Validation, LEAR appointment and Financial Capacity Assessment [25] " and in the instructions indicated in the Application Form Part B template.

8.1 Financial capacity

Applicants must have stable and sufficient sources of funding to maintain their activity throughout the duration of the grant and to participate in its funding. The applicants' financial capacity will be assessed on the basis of the supporting documents requested by the Commission services:

a) Low value grants (≤ EUR 60 000):
   - a declaration on their honour.

[22] Established in line with Council Regulation (EEC) No 2137/85 of 25 July 1985 – the European Economic Interest Grouping, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al26015

[23] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Text with EEA relevance), see http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32009L0072

[24] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (Text with EEA relevance), see http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32009L0073

[25] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/lev/h2020-rules-lev-lear-fvc_en.pdf

b) Grants > EUR 60 000:
   - a declaration on their honour, and
   - the profit and loss account as well as the balance sheet for the last 2 financial years for which the accounts were closed;
   - for newly created entities: the business plan might replace the above documents;

c) Grants for an action > EUR 750 000:
   (i) the information and supporting documents mentioned in point b) above, and
   (ii) **an audit report** produced by an approved external auditor certifying the accounts for the last 2 financial years available, where such an audit report is available or whenever a statutory report is required by law.
   If the audit report is not available AND a statutory report is not required by law, a self-declaration signed by the applicant's authorised representative certifying the validity of its accounts for the last 2 financial years available must be provided.
   In the event of an application grouping several applicants (consortium), the above thresholds apply to each applicant.

More comprehensive information on the documents to submit can be found at:
http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/lev/h2020-rules-lev-lear-fvc_en.pdf

In the event that the beneficiary's financial capacity is not satisfactory, the pre-financing payment may be subject to the receipt of a financial guarantee for up to the same amount as the pre-financing payment to be made.

8.2 Operational capacity

Applicants must have the professional competencies and appropriate qualifications necessary to complete the proposed Action for which the grant is sought. To assess this capacity, applicants must provide the following documents:

- description of the profiles of the people primarily responsible for managing and implementing the Action (e.g. accompanied by a *curriculum vitae*);
- the organisation's activity reports for at least the last year;
- a list of previous actions and activities carried out in equivalent actions in related fields

If compliant with the above-mentioned requirements, information submitted by applicants who have benefited from CEF Telecom support since 2014 may be taken into account in the evaluation of their operational capacity.

9. AWARD CRITERIA

Proposals will be evaluated against the following award criteria, which are defined in Annex 2 of the 2019–2020 Work Programme. These three criteria are **Relevance**, **Quality and efficiency of the implementation** and **Impact and sustainability** and are described below:

Relevance

- Alignment with the objectives and activities required for the deployment of the Digital Service Infrastructure described in Chapter 3 of the Work Programme and priorities set in section 2 of the call text.
- Alignment and synergies with EU long-term policy objectives, relevant policies, strategies and activities at European and national level.

Quality and efficiency of the implementation

- Maturity of the proposed solution (e.g. in terms of contribution towards interoperability, connectivity, sustainable deployment, operation, upgrading of trans-European digital service infrastructures, use of common building blocks, coordination at European level) and/or integration with existing components of the DSI.
- Coherence and effectiveness of the work plan, including appropriateness of the allocation of tasks and resources.
- Quality and relevant experience of the individual participants and, if more than one beneficiary, of the consortium as a whole (including complementarity, balance).
- Extent to which the proposal demonstrates support from national authorities, industry and NGOs (when relevant).
- Appropriate attention to security, privacy, inclusiveness and accessibility (when relevant).

Impact and sustainability

- Quality of the approach to facilitate wider deployment and take-up of the proposed Actions.
- Capability to survive, develop and scale up without European Union funding after the end of the project with a view to achieving long-term sustainability, where appropriate through funding sources other than CEF.

A score will be applied to each of the three award criteria on a scale from 0 (insufficient) to 5 (excellent). The threshold for individual criteria is 3. The overall threshold, applying to the sum of the three individual scores, is 10. Only proposals with a score on or above these thresholds (individual and overall) may be recommended for funding.

Ranking list

At the end of the evaluation by independent experts, all evaluated proposals will be ranked, according to the scores obtained for each of the award criteria as indicated above.

If necessary, a priority order for proposals which have obtained the same score within a ranked list will be determined. The following approach will be applied successively for every group of *ex aequo* proposals[26] requiring prioritisation, starting with the highest scored group, and continuing in descending order:

[26] Proposals with the same overall score

i. Proposals submitted by organisations established in an eligible country which is not otherwise covered by more highly-ranked proposals, will be considered to have the highest priority (geographical coverage).
ii. Proposals identified under (i), if any, will be prioritised according to the scores they have been awarded for the Relevance criterion. When these scores are equal, priority will be based on scores for the Impact and Sustainability criterion.

If a distinction still cannot be made, further prioritisation may be done by considering how to enhance the quality of the project portfolio through synergies between proposals, or other factors related to the objectives of the call or to the CEF Work Programme in general. These factors will be documented in the evaluation report.

10. LEGAL COMMITMENTS

In the event of a grant awarded by the Commission, the applicant(s) will be invited by INEA to sign a grant agreement drawn up in euro and detailing the conditions and level of CEF funding, as well as the information on the procedure to formalise the agreement of the parties. The standard model grant agreement, available on the call page, is not negotiable and will be signed in English.

Submitting an application implies the acceptance of the terms and conditions of the model grant agreement. Applicants are recommended to carefully read this document and its annexes before submitting an application.

A coordinator must be designated for multi-beneficiary Actions. The coordinator will be the contact point for INEA and will have, *inter alia*, the responsibility for receiving the payment(s) and coordinating the reporting exercise(s). It is strongly recommended that beneficiaries sign an internal cooperation agreement regarding their operation and coordination, including all internal aspects related to the management of the beneficiaries and the implementation of the Action.

Two copies of the original agreement must be signed first by the beneficiary in case of mono-beneficiary grants or the coordinator on behalf of the consortium and returned to INEA immediately.

In accordance with Article 23 of the CEF Regulation, only Actions in conformity with EU law, in particular in the area of public procurement, and which are in line with the relevant EU policies in the area of telecommunications infrastructure shall be financed.

11. FINANCIAL PROVISIONS

11.1 Forms of the grant

11.1.1 Reimbursement of costs actually incurred[27]

[27] Notwithstanding the form of grant, personnel costs may be declared on the basis of average costs calculated in accordance with the beneficiary's usual costs accounting practices, in compliance with the conditions laid down in Commission Implementing Decision C(2016)478 on the reimbursement of personnel costs of beneficiaries of the Connecting Europe Facility.

The grant will be defined by applying a maximum co-financing rate of 75% to the eligible costs and which 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’) for the following categories of costs: indirect costs minus subcontracting costs within the meaning of Article II.10 and costs of financial support to third parties within the meaning of Article II.11 ("reimbursement of flat-rate costs").

For details on eligibility of costs, please refer to section 11.2.

11.2 Eligible costs

Eligible costs are costs actually incurred by the beneficiary of a grant, which meet all the criteria laid down in Article 186 of the Financial Regulation.

The beneficiary's internal accounting and auditing procedures must permit direct reconciliation of the costs and revenue declared in respect of the action with the corresponding accounting statements and supporting documents.

The same criteria apply to the costs incurred by designated affiliated entities and implementing bodies.

Applicants' attention is drawn to points (3) to (8) of Article 8 of the CEF Regulation concerning the eligibility of costs. The full costs of purchase of equipment and infrastructure which are treated as capital expenditure are eligible under this call.

Costs may be eligible at the earliest from the date on which an application is submitted[28].

VAT
In line with the first subparagraph of Article 8(7) of the CEF Regulation and Article 186(4) (c) of the Financial Regulation, VAT paid by beneficiaries of grants awarded following this call for proposals is eligible except:

- deductible VAT (VAT paid by the beneficiary for the implementation of taxed activities or exempt activities with right of deduction);
- VAT paid for the implementation of activities engaged in as a public authority by the beneficiary where it is a Member State, regional or local government authority of a Member State or another body governed by public law of a Member State.

Financial support to third parties
The applications may not envisage provision of financial support to third parties.

Detailed information on eligible and ineligible costs is included in Article II.19 of the model grant agreement, which is available on the call webpage.

[28] The date when the proposal was last submitted in the TENtec eSubmission module will be considered as the submission date of the proposal.

11.3 Reporting and payment arrangements

Actions will be eligible to receive a pre-financing of up to 60% of the maximum grant amount awarded that will be made within 30 days after the last party signs the grant agreement. No interim payment will be made.

In the event that the beneficiary's financial capacity is not satisfactory, the pre-financing payment may be subject to the receipt of a financial guarantee for up to the same amount as the pre-financing payment to be made.

The financial guarantee, in euro, must be provided by an approved bank or financial institution established in one of the EU Member States. When the beneficiary is established in a third country, INEA may agree that a bank or financial institution established in that third country may provide the guarantee if the bank or financial institution is considered to offer equivalent security and characteristics as those offered by a bank or financial institution established in a Member State. Amounts blocked in bank accounts will not be accepted as financial guarantees.

The guarantee may be replaced by a joint or several guarantees provided by third parties or by a joint guarantee of the beneficiaries of an action that are parties to the same grant agreement. The guarantee will be released when the pre-financing is cleared against the interim payment, if applicable, and/or the balance of payment(s) made, in accordance with the conditions laid down in the grant agreement.

The final amount of the grant to be awarded to the beneficiary is established after completion of the Action, upon approval of the request for payment including, where applicable, the supporting documents as described in the model grant agreement.

11.4 Other financial conditions

a) Non-cumulative award

An Action may only receive one grant from the EU budget.

To ensure this, applicants must indicate in the application the sources and amounts of EU funding received or applied for the same Action or part of the Action, as well as any other funding received or applied for the same Action.

In this respect, any proposed Action or part(s) thereof that receives or has received EU funding under the CEF or other EU Programmes (e.g. European Structural and Investment Funds (ESIF), Horizon 2020, etc.) will not be funded under this call.

b) Non- retroactivity

No grant may be awarded retrospectively for Actions already completed.

A grant may be awarded for an Action which has already begun only where the applicant can demonstrate in the grant application the need to start the Action before the grant agreement is signed.

In such cases, costs eligible for financing may not have been incurred prior to the date of submission of the grant application.

c) No-profit

In accordance with Article 192 of the Financial Regulation, grants shall not have the purpose or effect of producing a profit within the framework of the Action. Where a profit is made, INEA will be entitled to recover the percentage of the profit corresponding to the EU contribution to the eligible costs actually incurred by the beneficiary to carry out the Action.

12. PUBLICITY

12.1 By the beneficiary

Beneficiaries must clearly acknowledge the European Union's contribution in all publications or in conjunction with activities for which the grant is used.

In this respect, beneficiaries are required to give prominence to the name and emblem of the European Commission and the reference to the CEF Programme on all their publications, posters, programmes and other products realised under the co-financed project.

12.2 By the Commission

All information relating to grants awarded in the course of a financial year shall be published on an internet site of the European Union institutions no later than the 30 June of the year following the financial year in which the grants were awarded.

13. PROCESSING OF PERSONAL DATA

The reply to any call for proposals involves the recording and processing of personal data (such as name, address and CV). Such data will be processed pursuant to Regulation (EU) 2018/1725[29] on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. Unless indicated otherwise, the questions and any personal data requested that are required to evaluate the application in accordance with the call for proposal will be processed solely for that purpose by INEA.

Personal data may be registered in the Early Detection and Exclusion System by the Commission, should the beneficiary be in one of the situations mentioned in Articles 136 and 141 of the Financial Regulation. For more information see the Privacy Statement on: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity.

14. PROCEDURE FOR THE SUBMISSION OF PROPOSALS

[29] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39–98).

Proposals must be submitted by the deadline set out under section 3.

No modification to the application is allowed once the deadline for submission has elapsed. However, if there is a need to clarify certain aspects or to correct clerical mistakes, the Commission may contact the applicant during the evaluation process.

Applicants will be informed in writing about the results of the selection process.

All practical information on this call for proposals and the evaluation process is detailed in the Guide for Applicants. It is available, together with the application forms, model grant agreement, the 2019–2020 Work Programme, and other relevant documents on the call webpage: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity.

Applicants are requested to carefully read all call-related documents, including the detailed instructions given in the Guide for Applicants on how to complete their applications and other guidance documents and information, in particular the Frequently Asked Questions (FAQ).

14.1 Application forms

Proposals must be submitted using the application forms provided on the call webpage at the link above. Applicants are strongly encouraged to submit their applications in English.

Proposals must be signed by the applicant(s) or its duly authorized representative and must be perfectly legible so that there can be no doubt as to words and figures.

The applicant(s) specified in application form part A will automatically be considered as the beneficiary(ies) if the proposal is selected for funding. If applicants designate affiliated entities within the meaning of Article 187 of the Financial Regulation to support the implementation of the submitted Action, information on these affiliated entities must be encoded in application form part A, and any relevant supporting documents must be provided.

For multi-applicant proposals, a coordinating applicant must be designated.

14.2 Submission process

Proposals must be submitted electronically using the TENtec eSubmission module, accessible via the following link:
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

before the call deadline: **5 November 2020 at 17:00.00 Brussels time** *(see also section 5 on Admissibility requirements).*

Application form part A is automatically generated by the eSubmission module. Application form parts B, C and D must be downloaded from the call webpage at the link above and duly completed. Once final, these must be uploaded into the TENtec eSubmission module. The same applies to any other annexes or supporting documents accompanying the proposal.

Applicants' attention is drawn to the fact that for application form part A, only the information encoded in the TENtec eSubmission module will be taken into account for the evaluation (notwithstanding the requirement to upload signed versions of application forms part A2.2 and A2.3). For the other forms and documents, only the last version uploaded in the TENtec eSubmission module will be taken into account for the evaluation.

Any parts of the application that require signatures of applicants or relevant authorities must be scanned and uploaded into the TENtec eSubmission module. Applicants must be able to provide the original documents and send them to the INEA services upon request.

Advanced electronic signatures based on a qualified certificate[30] as defined by the eIDAS Regulation[31] and which comply with the signature formats specified in Commission Implementing Decision 2015/1506 will be accepted. If a document is e-signed, a printable version of the document must be uploaded in the TENtec eSubmission module.

15. INFORMATION FOR APPLICANTS

Further information or clarifications on the call for proposals will be published on the call webpage. Please refer to all of the following documents, available on the call webpage, when preparing the application:

- 2019–2020 Work Programme
- CEF Regulation
- Telecom Guidelines
- Application form (Parts A, B, C and D)
- Guide for Applicants
- FAQs published on the call page
- Model grant agreement
- Checklist of documents to be provided
- EU Financial Regulation
- Commission Decision on the reimbursement of personnel costs

Applicants are recommended to consult the webpage and the INEA website/Twitter feed (@inea_eu) regularly until the deadline for submission of proposals.

Questions related to this call must be addressed to the call helpdesk:
INEA-CEF-Telecom-Calls@ec.europa.eu.

The answers to submitted questions will be published in a FAQ list accessible via the call webpage, to ensure equal treatment of all potential applicants. Questions related to the call should be submitted at the latest by **15 October 2020** to ensure sufficient time for the last update of the FAQs by **29 October 2020**. However, individual technical questions related to TENtec eSubmission module will be treated until the call deadline.

Questions which are specific to a particular proposal and for which the answer would

[30] For a list of trusted certificate providers please see https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

[31] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

provide a comparative advantage to the applicant will not be answered.

Please note that proposals must not be sent to the helpdesk e-mail address.