APEL PENTRU PROPUNERI DE PROIECTE DE INTERES COMUN

PROGRAMUL COMUNITAR CEF TELECOM

AGENȚIA EXECUTIVĂ INOVARE ȘI REȚELE, COMISIA EUROPEANĂ[1]

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE, GUVERNUL ROMÂNIEI[2]

MINISTERUL FONDURILOR EUROPENE, GUVERNUL ROMÂNIEI[3]

Cod apel	**CEF - TC - 2019 – 2 Critical digital infrastructure support - CYBERSECURITY – Suport pentru infrastructuri digitale critice - Securitate Cibernetică** **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity**
Încadrarea în Manualul de Implementare Multianual CEF TELECOM 2019 - 2020	**Secțiunea 3.8 Critical digital infrastructures support – CYBERSECURITY a Manualului de Implementare Multianual CEF TELECOM 2019 - 2020[4]** Contextul general al acestui apel de propuneri (de proiecte) este definit în secțiunea menționată anterior a Manualului de Implementare Multianual CEF TELECOM 2019 – 2020, așa cum apare publicat pe pagina website-ului apelului de către Innovation and Networks Executive Agency (INEA)[5]. Background-ul și argumentarea pentru acest apel de propuneri (de proiecte) sunt definite în secțiuna 3.8.1. a Manualului de Implementare Multianual CEF TELECOM 2019 – 2020. Finanțarea prin intermediul apelului își propune să faciliteze îmbunătățirea capabilităților Statelor Membre în securitatea cibernetică, la fel ca și cooperarea. În mod particular, aceasta presupune implementarea efectivă a Security of Network and Information Systems Directive Directive (EU) 2016/1148 - "NIS

[1] *Agence exécutive pour l'innovation et les réseaux / Uitvoerend Agentschap innovatie en netwerken, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË – Tel. +32 22991111.*
https://ec.europa.eu/inea/en

[2] *https://www.comunicatii.gov.ro/*

[3] *http://mfe.gov.ro/*

[4] *Commission Implementing Decision C(2019)1021 final of 14 February 2019 on establishing a Multi-Annual Work Programme 2019 and 2020 for financial assistance in the field of Connecting Europe Facility (CEF) Telecommunications sector, amended by Commission Implementing Decision C(2019)2782 final of 16 April 2019*

[5] *https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity*

	Directive" și inițierea pașilor pentru susținerea cerficării stakeholderilor așa cum este prevăzut prin EU Cybersecurity Act[6]. Alte detalii privind acest apel de propuneri (de proiecte) pot fi consultate prin parcurgerea secțiunii 3.8. destinată Critical digital infrastructures support - Cybersecurity din cadrul Manualului de Implementare Multianual CEF TELECOM pentru 2019 - 2020, respectiv, paginile 40-42. **Legislația comunitară și / sau alte referințe comunitare** ce reglementează inițiativele finanțate prin acest apel de proiecte includ: -NIS Directive: **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** -NIS Directive Introduction: **https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive** -Cyber Security package: **https://ec.europa.eu/digital-single-market/en/cyber-security** -CEF Digital Single Web Portal: **https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home** -CEF Regulation: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R1316** -Telecommunications Regulation: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.086.01.0014.01.ENG** -EU Financial Regulation: **https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1046** -MODEL GRANT AGREEMENT UNDER THE CONNECTING EUROPE FACILITY (CEF) – TELECOMMUNICATIONS SECTOR: **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/beneficiaries-info-point** -Innovation and Networks Executive Agency, Data Protection Notice for data subjects involved in grant award procedures: **https://ec.europa.eu/inea/sites/inea/files/data_protection_notice-inea1-cef-grant.pdf** -Commission Decision on the reimbursement of personnel costs: **https://ec.europa.eu/inea/sites/inea/files/c_2016_478_f1_commission_decision_en_v2_p1_837603.pdf** **https://ec.europa.eu/inea/sites/inea/files/2016_cef_ec_decision_reimbursement_annex.pdf** -List of National Contact Points for CEF TELECOM:

[6] *Regulation (EU) 2019/881 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*

	https://ec.europa.eu/digital-single-market/en/connecting-europe-facility **-**Detalii privind **evaluarea și selecția**, alături de modalitatea de **transmitere a aplicațiilor propunerilor de proiecte** pentru: **CEF TELECOM 2019 CALLS FOR PROPOSALS CEF-TC-2019-2** • Cybersecurity • eHealth • eProcurement • European e-Justice • European Platform for Digital Skills and Jobs • Public Open Data se pot obține accesând următorul link: **Guide for Applicants Version 1.0 – 4 July 2019** **https://ec.europa.eu/inea/sites/inea/files/2019_2_guide_for_applicants_cef_telecom_final.pdf** **-Verificarea documentelor ce trebuie depuse** în accesarea acestor fonduri se poate realiza prin parcurgerea **Application checklist** **https://ec.europa.eu/inea/sites/inea/files/cef_tc_checklist_call_2019_2.pdf** **-Solicitările de clarificare** preluate din partea potențialilor beneficiari de către Comisia Europeană, prin intermediul Agenției INEA[7] (ce au putut fi adresate cu ocazia **Zilei Virtuale de Infomare CEF TELECOM** din data de **10 Iulie 2019,** sau, ce pot fi adresate prin intermediul **helpdesk-ului** deschis până cel târziu în data de **24 Octombrie 2019** la adresa de email **INEA-CEF-Telecom-Calls@ec.europa.eu) se colectează** și se **actualizează**, sub formă de **răspunsuri scrise**, prin intermediul secțiunii **Întrebări Frecvente - Frequently Asked Questions (FAQs),** **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-cef-telecom-frequently-asked-questions.** **Ultima actualizare** a Întrebărilor Frecvente - Frequently Asked Questions (FAQs) se va realiza în data de **7 Noiembrie 2019.** Întrebările care sunt specifice unei propuneri particulare, și pentru care răspunsul ar putea genera un avantaj comparativ pentru aplicant, **nu vor fi preluate.**
Obiective	Obiectivele acestui apel și activitățile pentru care se poate obține finanțare sunt descrise în paragrafele ce urmează. Fiecare propunere (de proiect) trebuie să fie adresată **numai unuia** din

[7] https://ec.europa.eu/inea/en

următoarele Obiective și trebuie să specifice clar cărui Obiectiv i se adresează.

Obiectivul 1: Cooperarea dintre CSIRT-urile nominalizate național (Computer Security Incident Response Teams) pentru utilizarea îmbinată a MeliCERT-urilor

Finanțarea va fi acordată ca un stimulent CSIRT-urilor naționale pentru participarea acestora la facilitatea mecanismului de cooperare a MeliCERT-urilor și, dacă este aplicabil, să își dezvolte capacitatea de securitate cibernetică. Detaliile software-ului MeliCERT sunt disponibile public[8].

Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să fie depuse de către un consorțiu format din cel puțin două CSIRT-uri naționale, nominalizate de un Stat Membru așa cum se solicită prin intermediul Directivei NIS[9]. Aceste CSIRT-uri naționale trebuie să se afle localizate în cel puțin două State Membre diferite.

Dacă nu s-a realizat deja astfel, aceste CSIRT-uri naționale sunt de așteptat să instaleze și să utilizeze MeliCERT-uri la scurt timp după începerea Acțiunii.

Propunerile (de proiecte) **trebuie să se adreseze** tipurilor de activități schițate mai jos – **amândoura**:

a) activități pentru completarea funcționalității facilității MeliCERT-urilor pentru a intensifica cooperarea rapidă și efectivă (între) hotarele transversale între diferite CSIRT-uri naționale. Aceasta trebuie să includă dezvoltarea și implementarea infrastructurii IT pentru a permite utilizarea îmbinată a MeliCERT-urilor pentru schimbul de informații, de exemplu, prin dezvoltarea îmbinată a instrumentelor software pentru MeliCERT-uri, prin îmbunătățirea accesului la MeliCert-uri, inventând (un) incident îmbinat manevrând procese ce se bazează pe MeliCERT-uri[10].
b) activități de construire a încrederii pentru intensificarea cooperării (între) hotarele transversale, de exemplu, organizarea unor exerciții cyber îmbinate sau împărtășirea cunoștințelor.

Numai dacă un CSIRT național nu a primit finanțare pentru CSIRT-uri prin Apelurile CEF TELECOM Cybersecurity din 2016, 2017 sau 2018[11], **propunerea sa (de proiect) ar putea de asemenea să solicite** activități pentru

[8] *Details of the MeliCERTes software are publicly available via two separate websites, namely at https://gitlab.com/csirt-csp/csp-platform and at https://github.com/melicertes. Further information about the facility is available to the designated CSIRTs through the CSIRTs Network portal, hosted by European Union Agency for Network and Information Security (ENISA).*

[9] *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, Official Journal of the EU L194 of 19 July 2016, p. 1–30: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC*

[10] *Pentru traducerea din Limba Engleză a fragmentului: „(…) by devising joint incident handling processes relying on MeliCERTes (…)", Obiectivul 1, litera (a) – finalul acestui paragraph de la pag, nr. 2 din textul apelului de propuneri (de proiecte) CEF – TC – 2 Cybersecurity, disponibil prin accesarea următorului link astfel:*
https://ec.europa.eu/inea/sites/inea/files/2019-2_cyber_security_call_text_final.pdf

[11] *See list of Actions funded here: https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/projects-by-dsi*

îmbunătățirea capabilităților sale cyber. Asemenea activități pot fi infrastructura sau soft-ul suport, de exemplu, dezvoltarea sau achiziționarea infrastructurii incluzând instrumentele software; dezvoltarea competențelor și suportul structural cuprinzând training și servicii, ambele pentru staff-ul CSIRT și ca parte a serviciului furnizat pentru clienții săi.

Propunerile (de proiecte) selectate pentru acest Obiectiv sunt de așteptat să demonstreze utilizarea prelungită a facilității MeliCERT-urilor pe întreaga durată a Acțiunii.

Obiectivul 2: Suport pentru Operatorii de Servicii Esențiale (OES) identificați pentru dezvoltarea capabilității și pentru organizarea Centrelor pentru Împărtășirea și Analiza Informației (ISACs)

Finanțarea va fi alocată ca un stimulent pentru Operatorii Esențiali de Servicii (OESs) pentru îmbunătățirea capabilităților acestora de a manageria securitatea lor cibernetică și de a raporta incidentele cyber către autoritățile relevante în conformitate cu legislația relevantă națională și legislația Europeană. Finanțarea va fi de asemenea alocată ca un stimulent pentru crearea Centrelor pentru Împărtășirea și Analizarea Informației (ISACs).

Propunerile depuse sub acest Obiectiv **trebuie** să includă cel puțin **un** OES, identificat astfel în conformitate cu Directiva NIS.
Propunerile **trebuie** să fie adresate **unui** tip **sau ambelor** tipuri de activități schițate mai jos:
a)**îmbunătățirea capabilităților interne pentru a îndeplini cerințele de Securitate și raportare conform legislației naționale și a (legislației) Uniunii Europene.** Exemplele includ evaluarea riscului, teste de penetrare și audituri pentru a obține o mai bună sesizare a nivelelor de maturitate a securității, exerciții și training intern. Propunerile (de proiecte) trebuie să explice clar cum cerințele de securitate și de raportare vor fi adresate prin activitățile propuse, și ar trebui să ia în considerare urmarea liniile documentației publicate de către Grupul de Cooperare NIS[12].
b)**organizarea unui Centru pentru Împărtășirea și Analizarea Informației (ISAC) de nivel national sau European** pentru intensificarea (stării de) pregătire a securității cibernetice a Operatorului de Servicii Esențiale pentru împărtășirea efectivă a informației și îmbunătățirea conștientizării situaționale. Un asemenea ISAC trebuie să fie limitat la scopul unei industrii de sector sau subsector așa cum este delimitat/definit în Anexa II a Directivei NIS sau pentru alte asemenea sectoare așa cum au fost acestea incluse de Statele Membre în cauză în propria lor implementare a Directivei NIS. Mai mult decât atât, ISAC-ul trebuie să fie prezidat de un OES, să fie reprezentativ pentru stakeholderii industriei, și să implice autoritățile publice.

[12] *Publications by the NIS Cooperation Group are available here:*
https://ec.europa.eu/digital-single-market/en/niscooperation-group

ISAC-urile implică în general împărtășirea structurată și voluntară a informației securizate între colegi de încredere din amândoi furnizorii și operatorii unui sector al unei industrii particulare. ISAC-urile pot sprijini cu (starea de) pregătire îmbunătățită a securității cibernetice, cu conștientizarea situațională, și cu dislocarea coordonată a vulnerabilității. Astfel de documente puse la dispoziție de către European Uniun Agency for Network and Information Security (ENISA)[13] trebuie să fie luate în considerare.

Aplicațiile din partea OES care furnizează servicii esențiale în mai mult de un Stat Membru sunt încurajate în mod particular, cum ar fi acelea din OES în sectorul bancar, infrastructurile pieței financiare sau sectoarele sănătății. Pentru acest caz aplicația trebuie să explice clar ce servicii sunt furnizate și unde.

Propunerile (de proiecte) finanțate prin acest Obiectiv sunt de așteptat să îmbunătățească (starea de pregătire) a aplicanților și conștientizarea situațională prin schimbul voluntar securizat de informații a riscurilor de securitate cibernetică, țintelor, vulnerabilităților și incidentelor.

Beneficiarii finanțați prin acest Obiectiv sunt de așteptat:

- fie să se alăture unui ISAC relevant de Nivel Sectorial European, sau
- să participe în evenimente de stabilire a unui ISAC relevant de Nivel European Sectorial organizat prin facilitățile manageriale ISAC (care este organizat de Comisia Europeană)[14] și să aibă utilizarea serviciilor suport ale acelui management.

Valoarea finanțării așteptată să fie alocată prin acest obiectiv este de **3 milioane EURO** dintr-un buget total pentru acest apel de **10 milioane EURO**.

Obiectivul 3: Suport pentru Autoritățile Naționale Competente (NCAs) și Punctele Unice de Contact (SPOCs) pentru a iniția legătura, obligațiile intrate în vigoare și reglementările definite/delimitate prin Directiva NIS

Finanțarea va fi acordată ca stimulent destinat Autorităților Naționale Competente (NCAs) și Punctelor Unice de Contact (SPOCs) pentru a-și prelua efectiv rolul așa cum a fost acesta definit prin Directiva NIS.

Propunerile (de proiecte) depuse pentru acest Obiectiv **trebuie** să includă cel puțin **o** Autoritate Națională Competentă (NCA) sau Punct Unic de Contact (SPOC).

Propunerile (de proiecte) **trebuie să se adreseze activităților de contruire a**

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

[14] *The ISAC facility manager is being set-up by the European Commission through a procurement contract (SMART 2018/1022), which has not yet been awarded. More information is available here:* https://ec.europa.eu/digital-single-market/en/news/call-tender-support-operators-essential-services-oes-eu .

capabilităților proprii/interne pentru a iniția legătura, obligațiile intrate în vigoare și reglementările definite prin Directiva NIS, de exemplu prin prefecționarea și specializarea (înaltă) a staff-ului pentru a prelua auditurile de securitate informațională, prin facilitarea interacțiunii cu Autoritățile Naționale Competente (NCAs) și cu alte State Membre.

În plus față de construirea (acestor) capabilități proprii/interne, propunerile pot fi adresate unei sau mai multor din următoarele activități:

a) **facilitarea raportării** de la OES-urile și Furnizorii de Servicii Digitale – Digital Service providers (DSPs) către Autoritățile Naționale Competente - NCA-uri și Punctele Unice de Contact SPOC-uri.
b) **interacțiuni structurate** între NCA-uri și SPOC-uri și OES-uri și DSP-uri; de exemplu, consultarea și implicarea stakeholderilor.

Beneficiarii finanțați prin acest Obiectiv este de așteptat să participe în activități și evenimente organizate de managerul facilitator al cooperării securității cibernetice pentru NCA-uri și SPOC-uri[15] (care este instituit de Comisia Europeană[16]) și să utilizeze serviciile suport ale acelui manager.

Obiectivul 4: Cooperare Trans-Europeană pentru colaborarea îmbinată efectivă a operațiilor de Securitate cibernetică și pentru construirea reciprocă a încrederii/ siguranței

Finanțarea va fi acordată ca stimulent pentru facilitarea cooperării susținute între Statele Membre pentru operațiuni comune de securitate cibernetică și pentru construirea încrederii / siguranței reciproce.

Propunerile (de proiecte) supuse analizei pentru acest Obiectiv **trebuie** depuse de un consorțiu (format) din cel puțin **două** instituții/organisme publice naționale certificate/încredințate cu nivel de securitate cibernetică națională. Aceste organisme trebuie localizate în cel puțin două State Membre diferite.

Propunerile (de proiecte) trebuie să includă activități de cooperare între Statele Membre pentru operații efective de securitate cibernetică comună și construirea încrederii / siguranței reciproce. Aceste activități de cooperare trebuie să faciliteze continuarea sau crearea unor relații transnaționale stabile.

Propunerile de proiecte **pot** fi adresate, dar **pot să nu** fie limitate la tipul de activități schițate mai jos:

a) dezvoltarea ulterioară și implementarea cadrului operațional al European

[15] *The ISAC facility manager is being set-up by the European Commission through a procurement contract (SMART 2018/1022), which has not yet been awarded. More information is available here:* https://ec.europa.eu/digital-single-market/en/news/call-tender-support-operators-essential-services-oes-eu

[16] *The Cybersecurity Cooperation facilitation manager is being set-up by the European Commission through a procurement contract (SMART 2018/1023), which has not yet been awarded. More information is available here:* https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4426

Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises[17] – de exemplu, prin exerciții cibernetice

b) schimbul securizat de informații despre riscuri, ținte, vulnerabilități și incidente de securitate cibernetică
c) inițiative reciproce de creștere a conștientizării pentru industrii și (sectorul) public
d) răspunsuri reciproce cibernetice rapide, monitorizarea țintei hibride, inițiative reciproce de sprijin.

Beneficiarii finanțați prin acest Obiectiv este de așteptat să participe în activități și evenimente organizate de managerul facilitator al cooperării securității cibernetice pentru NCA-uri și SPOC-uri[18] (care sunt instituite de Comisia Europeană) și pentru utilizarea serviciilor suport ale acelui manager.

Obiectivul 5: Suport în certificarea securității cibernetice pentru un nivel comun de maturitate

Finanțarea va fi acordată pentru acest Obiectiv ca un stimulent pentru îmbunătățirea capabilităților și cooperării entităților care au responsabilitatea primară/principală/elementară pentru certificarea securității cibernetice la nivel national, pentru a facilita implementarea EU Cybersecurity Act.[19]

Propunerile (de proiecte) depuse pentru acest Obiectiv **trebuie** să includă cel puțin **o** entitate care are responsabilitatea primară/principală/elementară pentru certificarea securității cibernetice la nivel național. În cazul unor propuneri (de proiecte) cu mai mulți aplicanți, entitățile care aplică trebuie să fie localizate în cel puțin două State Membre diferite.

Propunerile (de proiecte) **pot** fi adresate, dar **nu pot** fi limitate la tipurile de activități schițate mai jos:

a) construirea capabilităților interne pentru preluarea efectivă a obligațiilor de certificare a autorităților naționale cu responsabilități în certificarea securității cibernetice, așa cum a fost definită/delimitată în EU Cybersecurity Act, de exemplu prin perfecționarea și specializarea înaltă a staff-ului pentru dezvoltarea propriilor capabilități de perfecționare. Asemenea perfecționări pot să pornească de la (aspecte) tehnice (de exemplu, cum să fie utilizate echipamentul de testare) până la aspecte

[17] https://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2017&number=6100&version=ALL
[18] *The Cybersecurity Cooperation facilitation manager is being set-up by the European Commission through a procurement contract (SMART 2018/1023), which has not yet been awarded. More information is available here:* https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4426
[19] *Regulation (EU) 2019/881 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

	mult mai generale (de exemplu, cum să redacteze profile ecranate/întărite, raporturi certificate). b) **sporirea capabilităților operaționale pentru certificare** prin achiziție și interoperabilitatea echipamentului relevant și a infrastructurii (de exemplu, echipament pentru testarea sistemelor IT cum ar fi pentesting, suport IT pentru facilitarea analizării documentației). c) **schimbul celor mai bune practici**, schimbul informației relevante privind certificarea, și suport (în) echipă privind certificarea securității cibernetice, de exemplu, privind aspecte tehnice despre organizarea auditurilor pentru evaluarea conformității organismelor. Asemenea schimburi pot să pornească de la programe de schimburi de personal până la crearea unor validări – expert a bazelor de date de bună practică. Beneficiarii finanțați prin acest Obiectiv este de așteptat să contribuie la activități și grupuri de lucru ale European Cybersecurity Certification Group stabilit conform EU Cybersecurity Act. Valoarea finanțării așteptată să fie alocată prin acest obiectiv este de **1 milion EURO** dintr-un buget total pentru acest apel de **10 milioane EURO**.
Solicitanți eligibili pentru acest apel de proiecte	**Compoziția Consorțiului și Entitățile eligibile**: -În conformitate cu Manualul de Implementare Multianual CEF TELECOM pentru anul 2019 – 2020, pag. 42 și fișa apelului de proiecte Cybersecurity[20], coroborat cu aplicarea Art. 9 din REGULAMENTUL CEF[21], numai acele propuneri de proiecte depuse de următoarele tipuri de aplicanți sunt eligibile: -Unul sau mai multe **State Membre**; -Cu acordul Statului/Statelor Membre țărilor EEA în cauză, organizații internaționale, alte consorții (Joint Undertakings[22]) sau întreprinderi publice sau private sau entități stabilite în Statele Membre. **Compoziția Obligatorie a Consorțiului** **Pentru Obiectivul 1:** Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să fie depuse de un consorțiu (format) din cel puțin două CSIRT-uri naționale, desemnate de un Stat Membru așa cum este solicitat prin Directiva NIS:

[20] https://ec.europa.eu/inea/sites/inea/files/2019-2_cyber_security_call_text_final.pdf

[21] *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/legalcontent/EN/TXT/?uri=CELEX%3A32013R1316

[22] *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* http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A12012E%2FTXT

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, Official Journal of the EU L194 of 19 July 2016, p. 1–30:
http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC .

Aceste CSIRT-uri naționale trebuie să fie localizate în cel puțin două State Membre diferite.

Pentru Obiectivul 2: Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să includă cel puțin un Operator de Servicii Esențiale (OES) identificat de Statele Membre în contextul Directivei NIS. Toate OES-urile trebuie să downloadeze de pe pagina apelului:

https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity ,

să completeze și să uploadeze ca document suport o scrisoare suport, care să fie semnată de Ministerul/Autoritatea națională relevantă prin care să se declare (faptul) că aplicantul este sau este în proces de a fi identificat drept OES. Acolo unde același Minister / Autoritate Națională este responsabil/responsabilă cu identificarea câtorva aplicații ca OES, este posibilă depunerea unei singure scrisori de suport prin care să se listeze toți aplicanții relevanți.

Dacă propunerea lor este reținută pentru finanțare, entitățile în procesul de a fi identificați ca OES la momentul depunerii vor trebui să își demonstreze statutul ca OES înainte de semnarea contractului de finanțare (pentru care sunt oferite detalii privind perioada estimativă de desfășurare a acestui proces în secțiunea Calendar Indicativ din prezentul document). Această cerință trebuie îndeplinită în perioada de timp specificată; altfel, Agenția INEA își rezervă dreptul de a închide procesul de pregătire a contractului de finanțare.

Pentru Obiectivul 3: Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să includă cel puțin o Autoritate Națională Competentă (NCA) sau un Punct Unic de Contact (SPOC) desemnat de Statul Membru conform prevederilor Directivei NIS.

Pentru Obiectivul 4: Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să fie depuse de un consorțiu (format) din cel puțin două instituții/organisme certificate/încredințate cu nivel de securitate cibernetică națională. Aceste organisme trebuie să fie localizate în cel puțin două State Membre diferite.

Pentru Obiectivul 5: Propunerile (de proiecte) supuse analizei pentru acest Obiectiv trebuie să includă cel puțin o entitate care are responsabilitatea primară/principală/elementară pentru certificarea securității cibernetice la nivel național. În cazul unor propuneri (de proiecte) cu mai mulți aplicanți, entitățile care aplică trebuie să fie localizate în cel puțin două State Membre diferite. Toți aplicanții trebuie să downloadeze de pe pagina web a apelului: ***https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity***

să completeze și să uploadeze ca document suport o scrisoare de aprobare, care să fie semnată de Ministerul/Autoritatea națională relevantă prin care să se declare (faptul) că aplicantul are la momentul curent responsabilitatea primară/principală/elementară pentru certificarea securității cibernetice la nivel național.

Țările EEA

În conformitate cu secțiunea 5.3.1 din Manualul de Implementare Multianual CEF TELECOM 2019 – 2020, statele din cadrul European Free Trade Association (EFTA) care sunt membre ale European Economic Area (EEA) pot participa[23] la apelul de proiecte, chiar dacă acest lucru nu este menționat în mod explicit în textul Manualul de Implementare Multianual CEF TELECOM 2019 - 2020, având aceleași drepturi, obligații și cerințe de îndeplinit ca și Statele Membre ale Uniunii Europene. La momentul publicării acestui apel, aceste condiții se aplică numai Norvegiei și Islandei.

⚠ Pentru aplicanții din Marea Britanie: îi rugăm să fie conștienți de faptul că criteriile de eligibilitate trebuie să fie îndeplinite pe *întreaga* durată a grantului. Dacă Marea Britanie iese din Uniunea Europeană pe perioada grantului fără să finalizeze o înțelegere (contractuală) cu Uniunea Europeană prin care să se stipuleze în mod particular faptul că aplicanții Britanici continuă să rămână eligibili, aceștia vor fi excluși de la obținerea finanțării Europene (în timp ce se continuă, unde este posibil, participarea) sau li se va solicita să părăsească proiectul în baza Articolului II.16.3.1 (a) (schimbarea situației legale a beneficiarului) din Contractul de Finanțare[24].

[23] *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.*

[24] *The model grant agreement is available on the call webpage:*
https://ec.europa.eu/inea/connecting-europefacility/cef-telecom/apply-funding/2019-cybersecurity
According with the Call Text – section 10. Legal Commitments, „The standard model grant agreement, available on the call page, is not negotiable and will be signed in English".

Țările Terțe și Entitățile din Țări Terțe

Atunci când este necesar să fie atinse obiectivele unui proiect de interes comun dat, și acolo unde este absolut motivat, Țările Terțe și entitățile stabilite în Țări Terțe pot participa la acțiuni ce contribuie la proiectele de interes comun. Acestea pot să nu primească finanțare conform prevederilor REGULAMENTULUI CEF, cu excepția situației în care este absolut indispensabil să fie atinse altfel obiectivele unui proiect de interes comun dat.

Statele în curs de aderare sau statele candidate beneficiind de o strategie de pre-aderare pot, de asemenea, să participe pentru acest sector al CEF ce cuprinde infrastructura de telecomunicații în conformitate cu Contractele de Finanțare semnate cu Comisia Europeană.

Cum la momentul lansării acestui apel de proiecte asemenea contracte de finanțare nu au fost semnate, aceleași condiții pentru Țările Terțe se aplică și statelor în curs de aderare și statelor candidate.

Țările Terțe și entitățile stabilite în Țările Terțe pot să participe numai ca parte a unui consorțiu cu aplicanți din state EU/EEA. Aplicația trebuie să conțină consimțământul Statului Membru în cauză ce susține Acțiunea propusă, precum și o declarație din partea partenerului European implicat în aplicația de proiect prin care să detalieze de ce este absolut indispensabilă participarea unei Țări Terțe.

Aplicanții care sunt entități stabilite într-o Țară Terță trebuie, de asemenea, să furnizeze o dovadă a susținerii proiectului lor din partea autorităților ce au sub incidența lor acțiunea.

Aplicanții fără personalitate juridică

Propunerile pot fi depuse de entități care nu au personalitate juridică (“do not have legal personality”) conform prevederilor legislației naționale, prin dovedirea faptului că reprezentanții lor dispun de capacitatea de a-și îndeplini obligațiile legale în locul lor și prin oferirea unei garanții pentru protejarea intereselor financiare ale Uniunii Europene care să fie echivalentă cu cea oferită de entitățile care au personalitate juridică (“legal persons”).

Persoanele Fizice

Propunerile depuse de Persoane Fizice nu sunt eligibile.

Entitățile Afiliate

	Aplicanții pot desemna entități afiliate în sensul prevederilor Art. 187 din REGULAMENTUL FINANCIAR cu scopul de a susține implementarea acțiunii depuse pentru finanțare. Asemenea entități afiliate trebuie să îndeplinească criteriile de eligibilitate pentru aplicanți. **Acordul Statului Membru** Orice aplicant care nu poate să furnizeze dovada acordului Statului Membru sau Țărilor din EEA nu poate fi eligibil.
Mecanisme de identificare a potențialilor parteneri ce formează consorții în accesarea fondurilor CEF TELECOM	Pentru mai multe detalii, a se accesa următorul link: **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity,** respectiv, **https://www.linkedin.com/m/login/**
Durata de desfăşurare a proiectelor de interes comun	-Durata indicativă a Acțiunii propuse prin intermediul acestui apel este de **3 ani.**
Buget apel	**Bugetul marcat pentru acest apel de proiecte este estimat la 10 milioane EURO pentru Servicii Generice.** -Valoarea finanțării așteptată să fie alocată prin Obiectivul 2: Suport pentru Operatorii de Servicii Esențiale (OES) identificați pentru dezvoltarea capabilității și pentru organizarea Centrelor pentru Împărtășirea și Analiza Informației (ISACs) este de **3 milioane EURO** dintr-un buget total pentru acest apel de **10 milioane EURO**. -Valoarea finanțării așteptată să fie alocată prin Obiectivul 5: Suport în certificarea securității cibernetice pentru un nivel comun de maturitate este de **1 milion EURO** dintr-un buget total pentru acest apel de **10 milioane EURO**. -Comisia își rezervă dreptul de a nu distribui toate fondurile disponibile. -Comisia își rezervă dreptul de a aloca un grant mai mic decât valoarea solicitată de aplicant. **-Aplicanții care au obținut deja fonduri prin apelurile anterioare CEF TELECOM Cybersecurity și care intenționează să aplice din nou, prin intermediul acestui apel, trebuie să explice în mod clar în secțiunea**

	relevantă din partea D a aplicației propunerii lor de proiect (în mod particular, în cadrul secțiunii 1 și/sau 2.1) modalitatea în care propunerea lor actuală de Acțiunea va construi asupra și/sau va diferi de acțiunea (acțiunile) finanțate prin apelul (apelurile) anterioare.
Valoarea finanțării acordate	-Granturi în valoare de până la **75%** din costurile eligibile.
Termen limită pentru avizarea anexelor în procesul de depunere a aplicațiilor și transmitere a documentelor către Agenția INEA	-Conform procedurilor aplicate de Organismul Intermediar pentru Promovarea Societății Informaționale (OIPSI) din cadrul Ministerului Comunicațiilor și Societății Informaționale și/sau de entitățile legale ale Guvernului României cu responsabilități în gestionarea secțiunii CEF TELECOM a **Programului Comunitar CEF ENERGIE, TELECOM, TRANSPORT**[25]. -Pentru mai multe detalii. A se vedea secțiunea „Alte Specificații" din prezentul document.
Calendar Indicativ[26]	Data publicării apelului pentru propunerile **CEF – TC – 2019 – 2: Cybersecurity**: **4 Iulie 2019** Termenul limită de depunere a propunerilor: **14 Noiembrie 2019**, orele **17:00.00** (Brussels time) Evaluarea propunerilor: Decembrie 2019 – Februarie 2020 (indicativ) Consultarea Comitetului CEF: Aprilie 2020 (indicativ) Informarea Parlamentului European: Mai 2020 Adoptarea Deciziei de Selecție: Mai 2020 (indicativ) Pregătirea și Semnarea Contractelor de Finanțare: între Mai 2020 și August 2020 (indicativ).

[25] *Pentru mai multe detalii, a se parcurge conținutul secțiunii:*
*„(...)**3.8.2.5 Governance, operations and stakeholders involvement***
A Governance Board was established as part of the WP 2014 preparatory action to focus on the DSI initiatives involving CSIRTs. Additional governance arrangements will be devised to meet the needs of the other stakeholders under this DSI, notably OES, DSPs, SPOCs, NCAs, CCAM entities, those involved in certification and other public bodies. The roles of the strategic and policy level NIS Co-operation Group and of the operational level CSIRTs Network will be examined to ascertain what added value these formal structures under the NIS Directive could provide as regards governance. (…)",
extrasă din cadrul:
*EUROPEAN COMMISSION, Brussels, 14.2.2019 C(2019) 1021 final ANNEX, „**ANNEX** to the **COMMISSION IMPLEMENTING DECISION on establishing a Multi-Annual Work Programme 2019 and 2020 for financial assitance in the field of Connecting Europe Pacility (CEF) Telecommunications sector**", 97 pages, correlated with EUROPEAN COMMISSION, Brussels, 16.4.2019, C(2019) 2782 final, CORRIGENDUM to Commission Implementing Decision C(2019)1021 final of 14 February 2019 on establishing a Multi-Annual Work Programme 2019 and 20202 for financial assistance in the field of Connecting Europe Facility (CEF) Telecommunications sector, and/or any updates of this call of proposal promoted by the European Commission as previously specified in this document.*

[26] *Toate **detaliile**, precum și **eventualele actualizări** ale apelului de proiecte **CEF TELECOM 2019 2: Cybersecurity** se regăsesc la nivelul paginii web cuprinzând apelul menționat:*
***https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity**,*
*alături de linkul pentru **CALL FOR PROPOSALS CONCERNING PROJECTS OF COMMON INTEREST UNDER THE CONNECTING EUROPE FACILITY IN THE FIELD OF TRANS-EUROPEAN TELECOMMUNICATION NETWORKS CEF TELECOM CALLS 2019 CEF-TC-2019-2: Cybersecurity**:*
***https://ec.europa.eu/inea/sites/inea/files/2019-2_cyber_security_call_text_final.pdf**.*

Documente utile	Documentația completă poate fi găsită la adresa paginii web a apelului de proiecte **CEF TELECOM 2019 – 2 Cybersecurity**: **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity** de unde pot fi parcurse/analizate/descărcate următoarele: **1.** Informații generale despre apel și atribuțiile Comisiei Europene în susținerea oricărui potențial beneficiar pentru accesarea fondurilor CEF TELECOM 2019 - 2, **2.** Calendarul Indicativ al Apelului, **3.** Manualul de Implementare Multianual CEF TELECOM 2019 - 2020, **4.** Documentele Apelului de Propuneri (inclusiv Modelul Contractului de Finanțare), **5.** Formularele pentru aplicare[27], **6.** Documente Suport, **7.** Documente și Informații Utile Comune pentru toate Apelurile (Documente de Background), **8.** Documente Specifice Apelului **Cybersecurity**. Înainte de depunerea propunerilor de proiecte este recomandat ca beneficiarii să consulte și legislația națională cu incidență asupra **Cybersecurity**, astfel încât să nu apară incompatibilități în diferitele faze de implementare ale aplicațiilor de proiecte. De asemenea, potențialii beneficiari care doresc să acceseze aceste fonduri pentru prima dată, precum și cei care au mai accesat fonduri CEF TELECOM prin intermediul apelurilor **Cybersecurity** anterioare, pot adresa solicitări de clarificare Agenției INEA, Comisia Europeană și pot vizualiza prezentările elaborate cu ocazia organizării **Zilei Virtuale de Infomare CEF TELECOM** din data de **10 Iulie 2019** – respectiv, prin urmarea actualizărilor de la nivelul următoarelor link-uri astfel: **https://ec.europa.eu/inea/en/news-events/events/2019-2-cef-telecom-call-virtual-info-day**

[27] *Pot fi downloadate pentru completare, prin accesarea următorului link, la secțiunea* ***Application Forms:***
Application Form Part A
For reference only: electronic submission of Part A using the eSubmission module is mandatory
Application Form Part B
Application Form Part C
Application Form Part D
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity

	și **https://webcast.ec.europa.eu/cef-telecom-2019-2-virtual-info-day-10-07-2019** În concluzie, pentru depunerea unei aplicații, este recomandat să se aibă în vedere: -parcurgerea conținutului apelului și a secțiunilor din Manualul de Implementare Multianual CEF TELECOM 2019 – 2020 care sunt relevante pentru apelul CEF TELECOM pentru care se va depune aplicația, precum și a CORRIGENDUMULUI C(2019) 2782 final, din 16.4.2019, menționat anterior pe parcursul acestui document; -parcurgerea și completarea formularelor necesare unei aplicații, **obținerea avizelor necesare de la nivel național**[28], consultarea Ghidului Aplicanților și a Întrebărilor Frecvente (FAQs), precum și urmărirea oricăror alte actualizări ale Comisiei Europene[29] ce pot apărea pe parcursul apelului de proiecte care vă interesează; -consultarea documentelor de background și a altor informații utile. Apoi **se poate aplica online** folosind **sistemul TENtec eSubmission**[30]: **https://webgate.ec.europa.eu/cas/login?loginRequestId=ECAS_LR-5285971-72uDjhtxarwIL36fbzYmI9zzwaG4zzQeINE272XZQf4fgK2Qpg1o6UyU0P7zSuvqELss9y4mZQPhpmPlu4pHBVzG-jpJZscgsw0K6JQjLd1mrOy-qUZXw6RI55TWuaC5EqybnbKaBqTg6zOx6pUpaDoqI42 .**
Alte specificații	Informații adiacente pot fi solicitate la numărul de fax: **021-311.39.19**, la numărul de tel. **021-311.41.12** sau la sediul Ministerului Comunicațiilor și Societății Informaţionale – **Organismul Intermediar pentru Promovarea Societăţii Informaţionale**, B-dul Libertății nr. 14, sector 5, București – având în vedere calitatea acestuia de Punct Național de Contact CEF TELECOM. Totodată, potențialii beneficiarii pot formula diferite solicitări de clarificare entităților legale ale Guvernului României sau unor alte entități legale care îi

*[28] Prin consultarea reprezentanților **Organismului Intermediar pentru Promovarea Societății Informaționale** – Ministerul Comunicațiilor și Societății Informaționale, care vă pot furniza **detalii** cu privire la **fluxul avizării la nivel național**.*

[29] Respectiv, la nivelul acestui link:
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity

[30] Modulul TENtec eSubmission este parte din Sistemul Informatic TENtec utilizat pentru managementul acțiunilor CEF pe întreaga durată a ciclului lor de viață, care facilitează depunerea electronică a propunerilor pentru apelurile CEF. Linkul către TENtec este disponibil la secțiunea „Application Forms" a paginii web destinată acestui apel de proiecte:
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity

	pot sprijini cu gestionarea la nivel național a prevederilor secțiunii **CEF TELECOM** din **Programul Comunitar CEF ENERGIE, TELECOM, TRANSPORT** - respectiv, **Critical digital infrastructure support - CYBERSECURITY** din cadrul Manualului de Implementare Multianual CEF TELECOM 2019 - 2020[31].

*

* *

[31] *EUROPEAN COMMISSION, Brussels, 14.2.2019 C(2019) 1021 final ANNEX, „**ANNEX** to the **COMMISSION IMPLEMENTING DECISION on establishing a Multi-Annual Work Programme 2019 and 2020 for financial assitance in the field of Connecting Europe Pacility (CEF) Telecommunications sector**”, 97 pages.*