MINISTERUL COMUNICAȚIILOR
ȘI
SOCIETĂȚII INFORMAȚIONALE

ROMÂNIA
1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

APEL PENTRU PROPUNERI DE PROIECTE DE INTERES COMUN

PROGRAMUL COMUNITAR CEF TELECOM

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE,

GUVERNUL ROMÂNIEI

MINISTERUL FONDURILOR EUROPENE, GUVERNUL ROMÂNIEI

AGENȚIA EXECUTIVĂ INOVARE ȘI REȚELE, COMISIA EUROPEANĂ

Cod apel:	**CEF – TC – 2018 – Apel 3** **Cyber Security** **https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security**
Încadrarea în Manualul de Implementare CEF TELECOM pentru anul 2018:	**Secțiunea 3.8.2.2.** a Manualului de Implementare CEF TELECOM pentru anul 2018. Toate Statele Membre ale Uniunii Europene sunt preocupate de soluționarea oricăror potențiale disfuncționalități legate de problematica cyber – security. Din această perspectivă, o bună cooperare între administrația publică și diferiți actori privați pe teme legate de vulnerabilități, riscuri, ținte și incidente în securitate va permite facilitarea condițiilor pentru furnizarea unor servicii de cyber – security de înaltă eficiență la nivelul spațiului comunitar. Prin urmare, posibilitatea de a dispune de o infrastructură de securitate cibernetică capabilă să facă față tuturor acestor problematici este esențială atât la nivel național, cât și comunitar. Detaliile generale privind acest apel de proiecte pot fi consultate prin parcurgerea secțiunii destinate Cyber Security din cadrul Manualului de Implementare CEF TELECOM, respectiv, 3.8. **Legislația comunitară** ce reglementează inițiativele finanțate prin acest apel de proiecte cuprinde în mod obligatoriu: -DIRECTIVA (UE) 2016/1148 A PARLAMENTULUI EUROPEAN ȘI A

	CONSILIULUI din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune – DIRECTIVA NIS; -Actualizări ale Pachetului destinat Securității Cibernetice din Septembrie 2017, prezentate din perspectiva impactului asupra Pieței Unice Digitale: https://ec.europa.eu/digital-single-market/en/cyber-security ; -Actualizările privind DIRECTIVA NIS pot fi parcurse prin accesarea următorului link: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive ; -Pachetul Cyber Security (Septembrie 2017): https://ec.europa.eu/digital-single-market/en/cyber-security; -CEF Regulation: Regulation (EU) No 1316/2013 of European Parliament and of the Council of 11 December 2013; -CEF Telecom Guidelines: 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; -Financial Regulation: Regulation (EU, EURATOM) No 966/2012 of the European Parliament and of the Council of 25 October 2013 as last amended by Regulation (EU, EURATOM) No 2015/1929 of 28 October 2015; -Rules of Application of the Financial Regulation: Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 as last amended by Commission delegated Regulation (EU) No 2015/2462 of 30 October 2015. Detalii privind modalitatea de **evaluare și selecție**, alături de modalitatea de **transmitere a aplicației cu propunerea de proiect** se pot obține accesând următorul link: https://ec.europa.eu/inea/sites/inea/files/cef_telecom_2018-2_2018-3_2018-5_guide_for_applicants_v2_15052018_final.pdf
Obiective:	**-Valoarea indicativă a acestui apel de proiecte este de 13,000,000 EURO și se acordă pentru Servicii Generice – Securitate Cibernetică.** **-Fiecare propunere trebuie să se adreseze numai unuia din Obiectivele acestui apel de proiecte și trebuie să specifice în mod clar cărui Obiectiv îi va fi adresată.**

	Obiectivul 1: Finanțările vor fi acordate sub formă de suport către CSIRT-urile desemnate de Statele Membre, așa cum sunt cerințele DIRECTIVEI NIS[1], pentru a-și dezvolta capacitățile de cyber security și pentru participarea lor la facilitatea mecanismului de cooperare MeliCERTes. Detaliile privind facilitatea MeliCERTes sunt disponibile pentru CSIRT-urile desemnate prin CSIRTs Network portal, găzduite de Agenția ENISA - (European Union Agency for Network and Information Security): https://www.enisa.europa.eu/ . Propunerile depuse în cadrul **Obiectivului 1**: -trebuie să cuprindă activități pentru facilitarea accesului de la nivelul CSIRTs-urilor naționale către facilitatea mecansimului de cooperare MeliCERTes, cum ar fi, de exemplu: integrarea sistemelor; testări; dezvoltarea sau achiziționarea de device-uri sigure și software, interfețe, porți de acces (gateways); transformarea mijloacelor locale în formate comune; -acolo unde este relevant, ar trebui să cuprindă, de asemenea, activități destinate pregătirii CSIRTs-urilor naționale, cum ar fi, de exemplu: dezvoltarea sau achiziționarea infrastructurii ce cuprinde mijloacele software; dezvoltarea abilităților și a suportului structural cuprinzând activități de training și servicii destinate agenților locali; dezvoltarea business case-urilor – cum ar fi, de exemplu, evaluarea și estimarea economică și financiară. Activitățile relevante pot să includă, însă nu trebuie neapărat să se limiteze la: -Infrastructură: achiziționarea și operarea la nivel național a sistemelor IT de securitate cibernetică; test – bed-urile experimentale încluzând infrastructura pentru nivelele de securitate; facilități de training; infrastructura Incidentelor în Securitate și Managementul Evenimentelor, honeypot-uri, sandboxes, mediile de simulare, alte componente software pentru automatizare, evaluarea riscurilor și a țintelor, managementul incidentelor și a evenimentelor, forensic computing și analize malware. -Abilități și dezvoltarea suportului structural: cursuri comune de training; “capture the

[1] *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, OJ L 194, 19.7.2016, 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*

	flag", "cybersecurity challenges"; "Red and Blue teaming", hackathons, exerciții cyber (incluzând evenimente la scară largă Europeană); campanii de conștientizare, asigurarea îndeplinirii condițiilor legale și analize organizaționale; managementul riscului; continuarea afacerii și planificarea pentru recuperare în urma dezastrelor. Propunerile selectate pentru acest Obiectiv este de așteptat să demonstreze interacțiunea cu sau utilizarea facilității MeliCERT-es până la sfârșitul acțiunii. **Obiectivul 2**: Dezvoltarea capabilității Operatorilor de Servicii Esențiale (Operators of Essential Services (OES)) și a Furnizorilor de Servicii Digitale (DSP) conform cu prevederile DIRECTIVEI NIS. Finanțarea va fi acordată OESs și DSPs, așa cum sunt aceștia definiți în DIRECTIVA NIS, sub formă de finanțare pentru dezvoltarea capacității lor de securitate cibernetică peste cerințele nivelului minim de securitate și raportare a cerințelor stabilite prin DIRECTIVA NIS. Pentru DSPs aceste cerințe sunt specificate mai detaliat în Commission Implementing Regulation laying down rules for application of the NIS Directive ((EU) 2018/151).[2] OESs avuți în vedere sunt aceea identificați sau în proces de a fi identificați de Statele Membre în contextul DIRECTIVEI NIS[3]. Propunerile care implică sectoarele transportului și energiei sunt în mod particular binevenite. DSPs avuți în vedere sunt acele entități ce cad sub incidența definiției Articolului 4(5) a DIRECTIVEI NIS. În mod corespunzător, serviciile digitale sunt definite ca " any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" of the type "online market place, online search engine and cloud computing service". [4]

[2] *Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, https://eur-lex.europa.eu/legalcontent/EN/TXT/?toc=OJ%3AL%3A2018%3A026%3ATOC&uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG*

[3] *Annex II of the NIS Directive references to specific sectors and subsectors for Operators of Essential Services.*

[4] *Article 4(5) of the NIS Directive refers to point (b) of Article 1(1) of Directive (EU) 2015/1535, and it further narrows the scope of the definition of digital services to the types of services listed in Annex III. In particular, Article 1(1) point (b) of Directive (EU) 2015/1535 defines these services as " any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services " and Annex III of the Directive narrows down the definition to three specific types of services: online market place, online search engine and cloud computing service. More information is available in the Communication from the Commission to the European Parliament and the Council "Making*

	Propunerile depuse prin intermediul acestui Obiectiv trebuie să cuprindă activități destinate pregătirii și dezvoltării OESs și DSPs – de exemplu, dezvoltarea sau achiziția de infrastructură ce cuprinde mijloace software; dezvoltarea abilităților și suport structural cuprinzând servicii și activități de training destinate agenților locali; schimburile de informații la nivel național / Information Sharing and Analysis Centres (ISACs); și dezvoltarea business case-urilor (cum ar fi, de exemplu, evaluarea și estimarea economică și financiară). Activitățile relevante pot să includă, dar nu ar trebui să se limiteze în mod necesar la: -Infrastructură: achiziționarea și operarea sistemelor de securitate cibernetică IT (Centrele Operaționale de Securitate, firewalls, detectarea intruziunilor / prevenție, monitorizarea echipamentului și software-ului); facilități de training; auto- evaluarea securității și raportarea toolkit-urilor; mijloace de auditare (evaluarea vulnerabilității, teste de penetrare); infrastructura Incidentelor în Securitate și Managementul Evenimentelor; honeypot-uri, medii de simulare; alte mijloace software pentru automatizare, evaluarea riscurilor și a țintelor, managementul incidentelor și al evenimentelor, forensic computing. -Abilități și dezvoltarea suportului structural: creșterea conștientizării staff-ului, campanii de conștientizare și cursuri de training; "capture the flag", schimbări legate de securitatea cibernetică, "Red and Blue teaming", hackathons, exerciții cyber (incluzând exerciții la scară largă europeană); analize organizaționale și asigurarea conformității legale; managementul riscului; asigurarea continuității afacerii și planificarea recuperării dezastrelor. Propunerile finanțate prin intermediul acestui Obiectiv sunt de așteptat să îmbunătățească pregătirea aplicantului și conștientizarea situațională prin schimbul voluntar securizat de informații privind riscurile, țintele, vulnerabilitățile și incidentele de securitate cibernetică. Beneficiarii vor fi așteptați să participe la mecanismul de cooperare pentru Information Sharing and Analysis Centres – ISACs la nivel sectorial European, care va fi stabilit de

the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52017DC0476

	Comisia Europeană pe parcursul perioadei 2018 – 2019. **<u>Obiectivul 3</u>:** Dezvoltarea capabilității în domeniul securității cibernetice pentru susținerea Cooperative Connected and Automated Mobility (CCAM) pentru sectoarele public și privat, în mod particular pentru automobilele electrice. Finanțarea va fi acordată pentru toți aplicanții eligibili din sectoarele public și privat în vederea dezvoltării capabilităților de securitate cibernetică în relația cu Cooperative Connected and Automated Mobility (CCAM), în particular, pentru vehiculele electrice. În contextul prezentului apel de proiecte, CCAM este de așteptat să acopere nivele de automatizare în condus 3, 4 și 5, așa cum sunt acestea definite de International Society of Automotive Engineers (SAE) - respectiv, SAE J3016 - Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems – și să acopere împreună: hardware-ul pentru infrastructura de drumuri, sistemele de telecomunicații 5G, vehiculele, controlul și navigația în trafic, precum și: facilitarea aplicațiilor software și fluxurilor de date. Securitatea cibernetică poate fi privită din perspectiva confidențialității, integrității și disponibilității atât pentru infrastructură cât și pentru siguranța facilitării datelor, mobilitatea eficientă și inteligentă. Propunerile depuse prin acest Obiectiv trebuie să aibă în vedere activități focusate pe dezvoltarea unor fluxuri de date mult mai rezistente și/sau flexibile și mai sigure, la fel ca și pentru creșterea pregătirii hardware-ului avut în vedere pentru reducerea vulnerabilităților și pentru a nu permite ținte și atacuri cibernetice. În mod particular, propunerile asociate accesului 5G de-a lungul coridoarelor transfrontaliere ale drumurilor, de specificat în propunerea de proiect, care implică vehicule conectate, automate, ar putea să furnizeze un feed back practic pentru riscurile și incidentele de securitate cibernetică. Activitățile relevante pot să includă, dar nu este necesar să se limiteze la: achiziționarea și operarea sistemelor IT de securitate cibernetică (Security Operations Centres, firewalls, detecția/prevenirea intruziunilor, monitorizarea echipamentului și a software-ului; facilitățile de training, toolkit-urile de raportare și auto evaluare a securității; mijloacele de auditare (evaluarea vulnerabilității, testarea penetrării); infrastructura Incidentelor de Securitate și Managementul Evenimentelor, honeypot-urile, mediile de simulare, alte mijloace software pentru automatizare, evaluarea riscului și a țintei, managementul incidentului și al evenimentului, forensic computing. În plus, propunerile pot avea în vedere abilități și dezvoltarea suportului structural:

	creșterea conștientizării staff-ului și cursuri de training; "capture the flag", cyber security challenges, "Red and Blue teaming", hackathons, exerciții de cyber (incluzând evenimente europene la scară largă); managementul riscului, continuitatea afacerii și planificările pentru acoperirea dezastrelor, precum și asigurarea conformității legale. Propunerile finanțate prin acest Obiectiv sunt de așteptat să îmbunătățească pregătirea și creșterea conștientizării aplicantului pentru schimburile voluntare de informații securizate privind riscurile de securitate cibernetică, ținte, vulnerabilități și incidente. Este de așteptat să participe la mecansime de cooperare de nivel European ISACs (Information Sharing and Analysis Centres) pentru CCAM ce vor fi stabilite de Comisia Europeană pe parcursul anilor 2018 – 2019. **Obiectivul 4**: Dezvoltarea capabilității National Competent Authorities (NCAs) și a Single Points of Contact (SPOCs) stabilite în conformitate cu prevederile DIRECTIVEI NIS. Finanțările vor fi acordate sub formă de sprijin către National Competent Authorities (NCAs) și Single Points of Contact (SPOCs) identificate de Statele Membre conform cerințelor DIRECTIVEI NIS, pentru dezvoltarea capacităților lor de securitate cibernetică, în vederea asumării efective a legăturii, reglementării și întăririi obligațiilor stabilite prin intermediul DIRECTIVEI NIS. Propunerile depuse sub acest Obiectiv trebuie să cuprindă activități pentru îmbunătățirea eficacității NCAs și SPOCs (de exemplu, dezvoltarea sau achiziționarea mijloacelor și abilităților pentru accesarea securității rețelelor și sistemelor informatice ale OES și DSPs, și pentru stabilirea suportului structural. Activitățile relevante pot cuprinde, însă nu este ablsolut necesar să se limiteze la: Infrastructură: achiziționarea și operarea test – bed-urilor experimentale incluzând scalări cibernetice, facilități de training; testarea securității produsului și certificarea echipamentului; securizarea camerelor de control; Laboratoare Specializate în certificarea Securității ICT în vederea testării produselor și serviciilor digitale; managementul riscului și mijloacelor de audit (evaluarea vulnerabilității, testarea penetrării), bazele de date pentru exploatare, vulnerabilitățile, notificările, raportările anuale, mediile de simulare, mijloacele software pentru evaluarea riscului și a țintei, managementul incidentelui și al evenimentului și forensic computing. Abilități și susținerea dezvoltării structurale: cursuri de training, exerciții de cibernetică

	(incluzând evenimente pe scară largă la nivel European), managementul riscului și auditarea; contorizarea bunelor practice; managementul conformității; analizele statistice și conformitate legală. Beneficiarii finanțați prin acest Obiectiv sunt de așteptat să participe la mecanismul de cooperare pentru notificarea și raportarea incidentelor în conformitate cu DIRECTIVA NIS, care vor fi stabilite de Comisia Europeană pe parcursul anilor 2018 - 2019. Prioritatea este asigurată pentru SPOCs, chiar dacă sunt sau nu NCAs. **Obiectivul 5**: Dezoltarea capabilității pentru autoritățile publice stabilite prin legislația națională sau europeană într-un Stat Membru pentru a respecta obiectivele de Politică a Uniunii Europene asociate cu Operational Level Cyber Security. Finanțările vor fi acordate ca suport către organismele publice stabilite legal de legislația națională sau europeană, care dispun de un contract de cooperare structurat cu cel puțin opt alte State Membre, pentru respectarea obiectivelor de politică ale Uniunii Europene asociate cu operațiunile de securitate cibernetică destinate creșterii conștientizării, a conștientizării situaționale, și a schimbului securizat de informații cu privire la riscurile de securitate cibernetică, ținte, vulnerabilități și incidente, sau răspunsul la incidente rapide. Propunerile finanțate prin acest Obiectiv trebuie să cuprindă activități pentru dezvoltarea platformelor IT destinate creșterii efective a conștientizării și conștientizării situaționale, alături de răspunsul prompt la incidente. Activitățile propuse pot include, dar nu trebuie să fie neapărat limitate la: Infrastructură: achiziționarea și operarea rețelelor IT într-o rețea de firme, portaluri web, test – bed-urilor experimentale incluzând scalări cibernetice; facilități de training; testarea securității produsului și certificarea ehipamentului; camere securizate pentru control; Laboratoare Specializate în certificarea Securității ICT pentru testarea produselor și serviciilor digitale; managementul riscului și mijloacele de audit (evaluarea vulnerabilității, testele de penetrare), bazele de date pentru exploatările, vulnerabilitățile, notificările, raportările anuale, simularea mediilor, mijloace software pentru evaluarea riscurilor și a țintelor, managementul incidentelor și al evenimentelor, forensic computing și analize malware. Abilități și dezvoltarea suportului structural: cursuri de training; exerciții de cibernetică

	(incluzând evenimente la scară largă europeană); managementul riscului și al auditului; păstrarea bunelor practici; conformitatea managementului; analizele statistice și conformitatea legală. Propunerile finanțate prin acest Obiectiv sunt de așteptat să îmbunătățească pregătirea și conștientizarea situațională a aplicantului prin schimbul voluntar securizat de informații privind riscurile de securitate cibernetică, țintele, vulnerabilitățile și incidentele. Este de așteptat ca beneficiarii să participe la mecanismul de cooperare pentru Centrele ISACS la nivel sectorial European (Information Sharing and Analysis Centres) ce vor fi stabilite de Comisia Europeană pe parcursul anilor 2018 – 2019.
Solicitanți eligibili pentru acest apel de proiecte:	**-Valoarea indicativă a acestui apel de proiecte este de 13,000,000 EURO și se acordă pentru Servicii Generice de Securitate Cibernetică - din care, 4,000,000 EURO vor fi destinați CCAM (Co-operative Connected and Automated Mobility).** **-Aplicanții care au obținut deja fonduri prin apelurile anterioare CEF TELECOM și își doresc să aplice din nou trebuie să explice în mod foarte clar în secțiunea 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 Acțiune diferă de acțiunea (acțiunile) finanțate prin apelurile anterioare – respectiv, prin detalierea acestor aspecte în "APPLICATION FORM, PART D – Technical Information"[5].** **- Fiecare propunere trebuie să se adreseze numai unuia din Obiectivele acestui apel de proiecte și trebuie să specifice în mod clar cărui Obiectiv îi va fi adresată.** -Conform prevederilor Manualului de Implementare CEF TELECOM pentru anul 2018 (pag. nr. 54) privind: *Compoziția Consorțiului: - se primesc propuneri din partea organizațiilor individuale - se primesc propuneri din partea consorțiilor.

[5] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security

	*Organizațiile eligibile sunt: - oricare. -În conformitate cu Manualul de Implementare CEF TELECOM pentru anul 2018 și în conformitate cu aplicarea **Art. 9 din REGULAMENTUL CEF TELECOM**[6], numai acele propuneri de proiecte depuse de unul dintre următorii aplicanți sunt eligibile: -Unul sau mai multe State Membre; -Cu acordul Statului/Statelor Membre sau a Țărilor EEA în cauză, organizații internaționale, alte consorții (Joint Undertakings[7]) sau consorții publice sau private sau entități stabilite în Statele Membre. **Eligibilitatea pentru Obiectivul 1**: -CSIRT-urile Naționale desemnate de Statele Membre în conformitate cu DIRECTIVA NIS. **Eligibilitatea pentru Obiectivul 2**: -Propunerile depuse pentru Obiectivul 2 trebuie să includă cel puțin un Operator de Servicii Esențiale (OES), sau, cel puțin, un Furnizor de Servicii Digitale (DSP): -OES țintă reprezintă acele entități identificate sau în curs de a fi identificate de Statele Membre în contextul DIRECTIVEI NIS. Toate OES-urile trebuie să download-eze de la nivelul paginii web a apelului de proiecte[8], să completeze și să upload-eze în calitate de document suport scrisoare de suport care trebuie să fie semnată de Ministerul relevant / Autoritatea Națională relevantă, prin care să se declare faptul că aplicantul este (deja) sau este în proces de a fi identificat ca OES. Acolo unde același Minister / Autoritate Națională este responsabil / responsabilă pentru identificarea mai multor aplicanți ca OES, este posibilă depunerea unei singure scrisori de suport care să cuprindă listarea tuturor aplicanților relevanți.

[6] *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, pentru mai multe detalii, se poate accesa acest link: http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32013R1316*

[7] *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, pentru mai multe detalii, se poate accesa acest link: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A12012E%2FTXT*

[8] *https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security*

	Entitățile în proces de a fi identificate ca OES în momentul depunerii vor trebui să confirme statutul lor ca OES dacă propunerea lor va fi reținută pentru finanțare. -DSP-urile țintă sunt acele entități ce cad sub incidența definiției Articolului 4 (5) din DIRECTIVA NIS. Articolul 4(5) din DIRECTIVA NIS se referă la punctul (b) al Articolului 1(1) al Directivei (EU) 2015 / 1535, și detaliează explicit scopul definiției serviciilor digitale ca tipuri de servicii care apar listate în Anexa III. În mod particular, Articolul 1(1) punctul (b) al Directivei (EU) 2015/1535 definește acele servicii ca fiind **"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"** și Anexa III a DIRECTIVEI stipulează definirea a trei tipuri specifice de servicii: **"online market place"**, **"online search engine"** și **"cloud computing service"**[9]. Toate DSPs trebuie să download-eze de pe pagina web a apelului de proiecte[10], să completeze și să upload-eze în calitate de document suport auto-declarația prin care DSPs îndeplinesc definiția DSP așa cum este aceasta stabilită prin DIRECTIVA NIS. **Eligibilitatea pentru Obiectivul 3**: nu se fac referințe privind condițiile de eligibilitate pentru acest Obiectiv la nivelul secțiunii "6.Criterii de Eligibilitate" din fișa apelului de proiecte destinat Securității Cibernetice, document disponibil online[11]. **Eligibilitatea pentru Obiectivul 4**: -Autoritățile Competente Naționale (NCAs) și/sau Single Points of Contact (SPOCs) desemnate de Statele Membre în conformitate cu prevederile DIRECTIVEI NIS. **Eligibilitatea pentru Obiectivul 5**: -Propunerile depuse sub Obiectivul 5 trebuie să includă cel puțin o organizație publică stabilită în mod legal prin legislația națională sau europeană, care să aibă un contract de

[9] *More information on DSPs in the NIS Directive is available is available in the Communication from the Commission to the European Parliament and the Council "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476 .*

[10] *https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security*

[11] *https://ec.europa.eu/inea/sites/inea/files/2018-3_call_text_cybersecurity_final.pdf*

	cooperare structurat cu cel puțin opt alte State Membre.  Pentru aplicanții din Marea Britanie: trebuie 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 obținerii grantului fără să finalizeze un contract cu Uniunea Europeană prin care să se stipuleze în mod particular faptul că aplicanții Britanici continuă să rămână eligibili, va însemna că au fost înșelați să obțină finanțare europeană (în timp ce vor continua, atunci când este posibil, să participe) sau li se va cere să părăsească proiectul în baza Articolului II.16.3.1 (a) (schimbarea situației legale a beneficiarului) din Contractul de Finanțare[12]. **Țările EEA** În conformitate cu secțiunea 5.3.1 din Manualul de Implementare CEF TELECOM pentru anul 2018, statele din cadrul European Free Trade Association (EFTA) care sunt membre ale European Economic Area (EEA) pot participa[13] la apelul de proiecte, chiar dacă acest lucru nu este menționat în mod explicit în textul Manualului de Implementare CEF TELECOM pentru anul 2018, având aceleași drepturi, obligații și cerințe de îndeplinit ca și Statele Membre. Pe perioada publicării acestui apel, aceste condiții se aplică numai Norvegiei și Islandei[14]. **Țările Terțe și Entitățile din Țări Terțe** Atunci când este necesar să fie atinse obiectivele proiectului de interes comun în cauză, și acolo unde este absolut motivată, Țările Terțe și entitățile stabilite în Țări Terțe pot participa în acțiuni ce contribuie la proiectul de interes comun. Ele pot să nu primească finanțare conform prevederilor REGULAMENTULUI CEF, cu excepția situației în care este absolut indispensabil să fie atinse altfel obiectivele respectivului proiect de interes comun. Statele în curs de aderare sau statele candidate care au o strategie de pre-aderare pot, de asemenea, să participe pentru acest sector al infrastructurii de telecomunicații CEF TELECOM în conformitate cu Contractele de Finanțare semnate cu Comisia Europeană.

[12] *Modelul Contractului de Finanțare este disponibil pe pagina web a apelului de proiecte Cyber Security: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security .*

[13] *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 .*

[14] *Din perspectiva acestui apel de proiecte, Liechtenstein este considerat un stat terț.*

La momentul lansării acestui apel de proiecte, nici un astfel de contract de finanțare nu a fost semnat, astfel încât, aceleași condiții similare Țărilor Terțe se vor aplica și statelor în curs de aderare.

Țările Terțe și entitățile stabilite în Țările Terțe pot să participe numai ca parte a unui consorțiu cu aplicanți din state EU/EEA. Aplicația lor trebuie să conțină consimțământul Statului Membru ce susține acțiunea în cauză, alături de 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 această acțiune.

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 de a oferi o garanție 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. 122 (2) (b) din REGULAMENTUL FINANCIAR[15] cu scopul de a susține implementarea acțiunii

[15] *Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (i.e. "Financial Regulation"), see http://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=celex%3A32012R0966*

	depuse pentru finanțare. Asemenea entități afiliate trebuie să îndeplinească criteriile de eligibilitate pentru aplicanți. **Acordul Statului Membru** Nici un aplicant care nu poate să furnizeze dovada acordului Statului Membru sau Țărilor din EEA nu poate fi eligibil.
Durata maximă de desfăşurare a proiectelor de interes comun:	**24 luni**
Buget apel:	**13,000,000 EURO pentru întregul apel de proiecte, din care, 4,000,000 EURO vor fi destinați CCAM (Co-operative Connected and Automated Mobility).** -Se va finanța numai un grant per Stat Membru. Prioritatea va fi acordată entităților care nu au fost finanțate prin intermediul Apelurilor Cyber Security cu ocazia Programelor de Implementare CEF TELECOM pentu anul 2016 și 2017. Pentru acest Obiectiv, o finanțare de maxim **1,000,000 EURO** per propunere selectată va fi finanțată. - Pentru **Obiectivul 2**, sunt așteptate propuneri prin care se solicită o contribuție de **150,000 EURO**. - Pentru **Obiectivul 3**, sunt așteptate propuneri prin care se solicită o contribuție de **150,000 EURO**. - Pentru **Obiectivul 4**, o contribuție de până la **100,000 EURO** este de așteptat. - Pentru **Obiectivul 5**, o finanțare de maxim **300,000 EURO** per propunere selectată va

	fi finanțată.
Valoarea maximă a finanţării acordate:	-Granturi în valoare de până la **75%** din costurile totale 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 entităților legale ale Guvernului României cu responsabilități în gestionarea **Programului Comunitar CEF ENERGIE, TELECOM, TRANSPORT**. Pentru mai multe detalii se poate accesa secțiunea "Alte Specificații" din prezentul document.
Calendar Indicativ[16]:	Data publicării apelului pentru propunerile CEF – TC – 2018 – 3: Cyber Security: **3 Mai 2018** Deschiderea Sistemului de Depunere: **16 Mai 2018** Termenul limită de depunere a propunerilor: **22 Noiembrie 2018**, orele **17,00** (timpul Bruxelles-ului) Evaluarea propunerilor: Decembrie 2018 – Februarie 2019 (estimativ) Consultarea Comitetului CEF: Aprilie 2019 (estimativ) Adoptarea Deciziei de Selecție: Aprilie 2019 (estimativ) Pregătirea și Semnarea Contractelor de Finanțare: între Aprilie și August 2019 (estimativ).

[16] *Conform Call for Proposals documents: 2018 CEF Telecom Call for Proposals – Cyber Security, Call Text și Reference of the Official Journal of the EU (C155/10). Toate aceste documente și informații, precum și actualizările privind apelul de proiecte CEF-TC-2018-3: Cyber Security se regăsesc la nivelul paginii web cuprinzând apelul menționat, respectiv: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security*

Documente utile:	Documentația completă poate fi găsită la adresa paginii web a apelului de proiecte CEF – TC – 2018 – 3: Cyber Security: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security de unde pot fi parcurse/analizate/descărcate următoarele: 1. Informații generale despre apelul de proiecte și atribuțiile Comisiei Europene în susținerea oricărui potențial beneficiar pentru accesarea fondurilor CEF-TC-2018-3 2. Calendarul Indicativ al Apelului 3. Manualul de Implementare CEF TELECOM 2018 4. Documentele Apelului de Propuneri 5. Formularele pentru aplicare 6. Documente Suport 7. Documente și Informații Utile Comune pentru toate Apelurile 8. Documente Specifice Apelului Cyber Security. Înainte de depunerea propunerilor de proiecte, este recomandat ca beneficiarii să consulte și legislația națională cu incidență asupra **Securității Cibernetice**, astfel încât să nu apară incompatibilități în diferitele faze de implementare ale aplicațiilor de proiecte. De asemenea, potențialii beneficiari care au mai accesat fonduri CEF TELECOM prin intermediul apelurilor de proiecte anterioare, destinate **Securității Cibernetice**, pot adresa solicitări de clarificare Agenției INEA, Comisia Europeană și pot vizualiza prezentările elaborate cu ocazia organizării Zilei de Infomare CEF TELECOM din data de 17 Mai 2018 postate la nivelul următorului link astfel: https://ec.europa.eu/inea/en/news-events/events/2018-2-2018-3-and-2018-5-cef-telecom-calls-virtual-info-day
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 Informaționale – Organismul Intermediar pentru Promovarea Societății

	Informaţionale, B-dul Libertăţii nr. 14, sector 5, Bucureşti – având în vedere calitatea acestuia de Punct Național de Contact CEF TELECOM. Totodată, beneficiarii pot formula diferite solicitări de clarificare entităților legale ale Guvernului României care îi pot sprijini cu gestionarea la nivel național a prevederilor Programului Comunitar CEF ENERGIE, TELECOM, TRANSPORT și secțiunii destinate **Securității Cibernetice** din cadrul „Manualului de Implementare CEF TELECOM pentru anul 2018”.

*

* *