



MINISTERUL COMUNICAȚIILOR  
ȘI  
SOCIETĂȚII INFORMAȚIONALE



**APEL PENTRU PROPUNERI DE PROIECTE DE INTERES COMUN  
PROGRAMUL COMUNITAR CEF TELECOM**

**MINISTERUL COMUNICAȚIILOR ȘI PENTRU SOCIETATEA INFORMAȚIONALĂ,  
GUVERNUL ROMÂNIEI  
MINISTERUL FONDURILOR EUROPENE, GUVERNUL ROMÂNIEI  
AGENȚIA EXECUTIVĂ INOVARE ȘI REȚELE, COMISIA EUROPEANĂ**

<b>Cod apel:</b>	<b>CEF – TC – 2017 – Apel 2 Cyber Security - Securitate Cibernetică</b>  <a href="https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2017-cef-telecom-call-cyber-security-cef-tc-2017-2">https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2017-cef-telecom-call-cyber-security-cef-tc-2017-2</a>
<b>Încadrarea în Manualul de Implementare CEF TELECOM pentru anul 2017:</b>	<b>Secțiunea 3.7</b> a Manualului de Implementare CEF TELECOM pentru anul 2017  Prioritățile acestui apel au în vedere în mod particular secțiunea 3.7.2.2. a Manualului de Implementare CEF TELECOM și sunt destinate, în principal, să susțină <b>Servicii Generice</b> furnizate de <b>CERT-urile – Computer Emergency Response Teams</b> sau <b>CSIRT-urile – Computer Security Incident Response Teams – naționale</b> sau <b>guvernamentale</b> în toate Statele Membre.
<b>Obiective:</b>	Finanțarea va susține <b>CERT-urile – Computer Emergency Response Teams</b> și <b>CSIRT-urile – Computer Security Incident Response Teams naționale / guvernamentale</b> să creeze, mențină sau să își extindă capacitățile naționale pentru a implementa o varietate de servicii de securitate cibernetică, în scopul de a ajunge la un stadiu de pregătire care le va permite să participe la o <b>accesare egală a /exercițiu comun asupra, la nivelul Platformei de Servicii Centrale în Securitatea Cibernetică – Cyber Security Core Service Platform (participate in a equal footing in the Cyber Security Core Service Platform)</b> – în baza mecanismelor de cooperare definite în <b>Manualul de Implementare CEF TELECOM pentru anul 2015</b> .



Activitățile asociate acestui apel de proiecte ar trebui să acopere, pe cât de mult posibil, următoarele:

1. Activități destinate creșterii pregătirii **CERT-urilor – Computer Emergency Response Teams** și **CSIRT-urilor – Computer Security Incident Response Teams naționale / guvernamentale** (de exemplu, dezvoltarea sau achiziționarea unor mijloace mai bune pentru analiza, identificarea și detectarea țintelor, **conștientizarea campaniilor de importanță secundară (awareness campaigns ancillary)** destinate dezvoltării capacităților, evaluării maturității și **dezvoltării îmbunătățirii administrării (encompassing governance)**, asigurarea conformității legale, a serviciilor către toți agenții locali)

2. Stabilirea **punctelor de acces** de la structurile **n(naționale) / g (guvernamentale) CERT/CSIRT** către **Platforma Centrală de Servicii - Core Service Platform** prin mecanismele de cooperare (de exemplu, device-uri sigure și software, interfețe, gateways, traducerea mijloacelor locale în formate comune).

Pentru unul sau altul din aceste obiective, aceste activități ar putea include:

-achiziționarea și operaționalizarea la nivel național a sistemelor IT pentru securitatea cibernetică, **anvelope pentru testări experimentale (experimental tests beds)** și facilități de training, care vor susține cooperarea transfrontalieră a structurilor **n(naționale) / g (guvernamentale) CERT/CSIRT**, ce ar putea să fie completate cu seturi de mijloace specifice foarte sofisticate pentru domeniul securității cibernetice care ar susține în mod direct operațiile CERT / CSIRT (de exemplu, **mecanisme de securitate destinate să separe programele alate în rulare - sandboxes**, medii pentru simulare, infrastructuri de cercetare avansate și **controlul securizat al camerelor – secure control rooms**).

-angajarea de personal calificat, perfecționarea angajaților existenți, organizarea unor întâlniri pentru cooperare, exerciții destinate securității cibernetice de-a lungul Europei, **auditări ale conformității protecției datelor – data protection compliance audits**. Oricum, activitățile de diseminare incluzând organizarea unor workshop-uri și întruniri trebuie să fie planificate în conformitate cu activitățile **Rețelei CSIRT**, precum și a altor **CSIRTs/CERTs**, pentru a evita orice posibile suprapuneri.

Trebuie subliniat faptul că activitățile privind **funcționarea** organizațiilor (de exemplu, instalarea / **design-ul și organizarea centrelor de date – outfitting data**, activitățile de perfecționare și / sau sălile de ședință cu dusumea, sisteme electrice, aer condiționat, mobilier de birou, sisteme fizice de control al securității, senzori de incendii, cabluri de rețea și prize, etc.) nu vor fi finanțate la nivelul acestui apel de proiecte.



	<p>Pentru toate acțiunile selectate în cadrul acestui apel de proiecte care își propun o conectare la <b>Platforma Centrală de Servicii - Core Service Platform</b>, mecanismele de cooperare (menționate anterior), precum și demonstrarea interacțiunii prin utilizarea Platformei <b>reprezintă o necesitate</b>.</p>
<b>Solicitanți eligibili pentru acest apel de proiecte:</b>	<ul style="list-style-type: none"><li>-Una sau mai multe organizații</li><li>-Unul sau mai multe State Membre</li><li>-Structurile <b>n(naționale)/g (guvernamentale) CERT/CSIRT</b> sau <b>structurile sectoriale CERTs/CSIRTs</b>. Fiecare aplicant trebuie să prezinte o <b>confirmare scrisă</b> din partea <b>Ministerelor de resort ale Statelor Membre</b> cu privire la statutul aplicantului - dacă este <b>n/g CERT / CSIRT</b> sau dacă este <b>structură sectorială CERTs/CSIRTs</b>.</li><li>-Informații adiționale: maxim o propunere pe țară (dacă nu sunt fonduri disponibile); prioritatea va fi oferită organizațiilor care nu au beneficiat de granturi anterioare din partea Programului Comunitar CEF TELECOM pentru secțiunea Securitate Cibernetică.</li></ul>
<b>Durata maximă de desfășurare a proiectelor de interes comun:</b>	24 luni
<b>Buget apel:</b>	- 12 milioane €
<b>Valoarea maximă a finanțării acordate:</b>	-Până la <b>75%</b> din costurile totale eligibile, pentru o limită maximă de <b>1 milion de Euro pentru fiecare acțiune</b>
<b>Termen limită pentru avizarea anexelor în procesul de depunere a aplicațiilor și transmitere a documentelor către Agenția INEA:</b>	-Cu 15 zile înainte de termenul limită de depunere (cel târziu până la data de 06.09.2017) - Ministerul Comunicațiilor și Societății Informaționale – Organismul Intermediar pentru Promovarea Societății Informaționale.



<b>Calendar Indicativ:</b>	Deschiderea apelului de proiecte: <b>06 Mai 2017</b> Termenul limită de depunere la Comisia Europeană: <b>21 Septembrie 2017</b> Perioada de evaluare a aplicațiilor: Octombrie-Decembrie 2017 (estimativ) Consultarea Comitetului CEF: Ianuarie 2018 (estimativ) Adoptarea Deciziilor de Selecție: Februarie 2018 (estimativ) Pregătirea Semnării Contractelor de Finanțare: Iunie 2018 (estimativ)
<b>Documente utile:</b>	Documentația completă poate fi găsită la adresa de Internet de unde pot fi descărcate:  <a href="https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2017-cef-telecom-call-cyber-security-cef-tc-2017-2">https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2017-cef-telecom-call-cyber-security-cef-tc-2017-2</a>  <ol style="list-style-type: none"><li>1. Documentele Apelului de Proiecte</li><li>2. Referințe privind reglementări europene</li><li>3. Formularele de Aplicare (A,B,C,D)</li><li>4. Formulare pentru verificarea capacității financiare</li><li>5. Ghiduri și alte documente utile</li><li>6. Alte informații specifice pentru apelul de proiecte de interes comun.</li></ol>
<b>Alte specificații:</b>	Orice clarificări 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 Informaționale, B-dul Libertății nr. 14, sector 5, București.

\*

\*

\*