H O T Ă R Â R I A L E G U V E R N U L U I R O M Â N I E I

GUVERNUL ROMÂNIEI

H O T Ă R Â R E
privind aprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor de investiții aferente proiectului „Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente”

În temeiul art. 108 din Constituția României, republicată, și al art. 42 alin. (1) lit. a) din Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. 1. — Se aprobă Nota de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor de investiții aferente proiectului „Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente”, prevăzută în anexa care face parte integrantă din prezenta hotărâre.

Art. 2. — Finanțarea proiectului prevăzut la art. 1 se realizează din fonduri externe nerambursabile, în cadrul Planului național de redresare și reziliență, componenta 7 — Transformare digitală, investiția 12 — Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente, precum și de la bugetul de stat, prin bugetul Serviciului Român de Informații, în limita sumelor aprobate cu această destinație, conform programelor de investiții publice aprobate potrivit legii.

Art. 3. — Serviciul Român de Informații răspunde de modul de implementare a proiectului prevăzut la art. 1, potrivit prevederilor prezentei hotărâri.

PRIM-MINISTRU
ILIE-GAVRIL BOLOJAN

Contrasemnează:
Viceprim-ministru,
Marian Neacșu

Viceprim-ministru,
ministrul afacerilor interne,
Marian-Cătălin Predoiu

Viceprim-ministru,
ministrul apărării naționale,
Radu-Dinel Miruță

Secretarul general al Guvernului,
Ștefan-Radu Oprea

p. Directorul Serviciului Român de Informații,
Răzvan Ionescu

p. Ministrul investițiilor și proiectelor europene,
Răzvan Popescu,
secretar de stat

Ministrul economiei, digitalizării, antreprenoriatului și turismului,
Ambrozie-Irineu Darău

Ministrul finanțelor,
Alexandru Nazare

București, 23 decembrie 2025.
Nr. 1.162.

ANEXĂ

N O T Ă D E F U N D A M E N T A R E

referitoare la necesitatea și oportunitatea efectuării cheltuielilor de investiții aferente proiectului „Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente”

Scopul investiției

Consiliul Uniunii Europene a aprobat Planul național de redresare și reziliență al României (*PNRR*), conform art. 20 din Regulamentul (UE) nr. 241/2021 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență, adoptând Decizia de punere în aplicare a Consiliului din 29 octombrie 2021 de aprobare a evaluării Planului de Redresare și Reziliență al României, modificată prin Decizia de punere în aplicare a Consiliului din 17 noiembrie 2025.

În conformitate cu prevederile Regulamentului (UE) nr. 241/2021, ale Deciziei de punere în aplicare a Consiliului de aprobare a evaluării Planului de Redresare și Reziliență al României, Serviciul Român de Informații, prin Centrul Național Cyberint, realizează investiția 12 — „Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente” din cadrul Componentei 7 — Transformare digitală, aferentă PNRR.

Context

Prin componenta C7 — Transformare digitală din cadrul PNRR se contribuie la atingerea obiectivului României în ceea ce privește conectivitatea digitală.

Având în vedere contextul sociopolitic actual, proiectul finanțat în baza Contractului de finanțare nr. 760.004 din 12.12.2022 reprezintă un demers strategic esențial pentru România, având la bază atât impactul adus grupului-țintă de beneficiari, cât și adaptarea la evoluția complexă a amenințărilor cibernetice, măsură necesară pentru consolidarea capacității de protecție și reacție în fața incidentelor cibernetice care pot afecta infrastructurile informatice guvernamentale.

Pentru România, securitatea cibernetică reprezintă o prioritate națională orizontală, acoperind domeniile economice și de apărare și incluzând educația, formarea, exercițiile cibernetice specifice, activitățile de sensibilizare și apărarea cibernetică, urmărindu-se creșterea nivelului de securitate cibernetică a entităților publice și private care dețin infrastructuri cu valențe critice.

În contextul crizei provocate de COVID-19, la nivel global s-au intensificat și diversificat activitățile ostile din spațiul cibernetic. Actorii cibernetici utilizează contextul social actual pentru derularea de atacuri cibernetice, care au la bază tehnici de inginerie socială, inclusiv cu scopul de a afecta servicii din domenii-cheie (producție, transport și distribuție de gaze naturale și energie electrică, sănătate, administrație publică, educație, transporturi etc.) cu impact ridicat asupra bunei desfășurări a activităților curente de la nivel național.

Pentru respectarea restricțiilor impuse de pandemia de COVID-19, majoritatea instituțiilor publice și companiilor private au adoptat, în regim de urgență, modelul work from home (telemuncă), accesarea de la distanță a rețelelor acestor entități devenind o necesitate pentru desfășurarea activităților curente. Astfel, prin eliminarea interacțiunilor dintre angajați a fost diminuat riscul răspândirii excesive a virusului SARS-CoV2, însă a crescut riscul expunerii infrastructurilor TIC folosite la atacuri cibernetice.

Sistemele informatice, care gestionează majoritatea infrastructurilor cu valențe critice, reprezintă o țintă predilectă a atacurilor cibernetice. Atacurile asupra sistemelor informatice, aparținând unor instituții ale statului sau aflate în proprietate privată, devin mai periculoase și mai dificil de prevenit. Ele pot fi inițiate atât de grupări de criminalitate organizată care vizează, în cele mai multe cazuri, obținerea de resurse financiare, cât și de către state ostile, pentru obținerea unor avantaje strategice. În acest context, principalele provocări au fost reprezentate de securitatea informațiilor vehiculate și a canalelor de comunicații, precum și de adoptarea și aplicarea măsurilor necesare menținerii unui nivel optim de securitate cibernetică.

Pe de altă parte, având în vedere că la nivelul Uniunii Europene a fost demarat Programul Europa Digitală, care urmărește creșterea capacităților digitale prin implementarea de tehnologii de ultimă generație, la nivelul României se dorește alinierea la standardele impuse de la nivelul UE, prin creșterea gradului de digitalizare și interconectarea propriilor servicii digitale cu cele europene.

Având în vedere cele menționate anterior, este necesară extinderea și dezvoltarea la nivel național a mecanismelor de protecție împotriva atacurilor cibernetice în continuă evoluție, prin adoptarea de tehnologii de ultimă generație (artificial intelligence, machine learning etc.) care să asigure mijloacele defensive optime pentru toate domeniile de interes național.

Obiectivul investiției I12 îl reprezintă creșterea arealului de protecție, prin valorificarea know-how-ului deținut și prin promovarea de modele de bune practici în demersurile de asigurare a securității cibernetice, precum și creșterea rezilienței, o condiție esențială pentru succesul activităților de protecție a infrastructurilor critice. Reziliența infrastructurii este strâns legată de modul în care organizațiile își gestionează riscurile strategice, operaționale și financiare. Astfel, proiectul vizează creșterea gradului de securitate cibernetică a sistemelor de securitate deja implementate în cadrul instituțiilor publice/entităților beneficiare, precum și a interoperabilității sistemelor de securitate care urmează să fie implementate și integrate cu sistemul informatic existent, în ceea ce privește coroborarea informațiilor, colaborarea, analiza și reacția prin intermediul mecanismului computerizat pentru alertarea rapidă și diseminarea informațiilor în timp real.

Din punctul de vedere al securității cibernetice, Centrul Național Cyberint (*CNC*) operează un *SOC* (Security Operation Center), prin care oferă deja, încă din anul 2015, servicii de securitate cibernetică pentru instituții publice (de exemplu, din domeniul administrației publice, energetic, sănătății, finanțelor, educației și cercetării), în scopul securizării, modernizării și eficientizării activităților proprii, circumscrise domeniului TIC.

Acest SOC asigură securizarea rețelelor instituțiilor publice și protejarea datelor prelucrate și stocate. Rolul SOC al CNC este de a detecta, a analiza și a răspunde la incidentele de securitate cibernetică detectate în cadrul infrastructurilor cu valențe critice, prin exploatarea soluțiilor de securitate cibernetică. Pentru derularea de investigații cât mai aprofundate și mitigarea riscurilor de securitate cibernetică, CNC derulează activități specifice, precum: analiză forensic, analiză malware, audituri de securitate cibernetică și management al incidentelor de securitate cibernetică. În cadrul acestui SOC sunt analizate evenimentele de securitate generate de la nivelul serverelor, stațiilor de lucru, bazelor de date, aplicațiilor, site-urilor web sau de la nivelul echipamentelor de comunicație și securitate, în scopul identificării activităților anormale, precursoare ale incidentelor cibernetice, prin implementarea la nivel național a unui sistem de management centralizat (*SIEM*).

Personalul SOC cooperează cu echipele din cadrul infrastructurilor protejate pentru soluționarea rapidă a incidentelor de securitate.

În derularea activității, structura CERT-CNC cooperează cu *DNSC* (Directoratul Național de Securitate Cibernetică), instituție ce deține rolul de autoritate națională cu competențe la nivel național în transpunerea măsurilor și cerințelor de securitate din directivele NIS, în vederea creșterii securității rețelelor și sistemelor informatice ce susțin servicii esențiale.

Proiectul propus de către CNC are în vedere și acoperirea unor infrastructuri TIC cu valențe critice din domenii care nu se regăsesc actualmente în sfera de competență a DNSC, dar care prin rolul lor sunt importante pentru securitatea națională.

Având în vedere faptul că CNC desfășoară activități în scopul cunoașterii, anticipării, prevenirii și contracarării amenințărilor la adresa infrastructurilor critice, proiectul propus cuprinde și infrastructuri *OT* (Operational technology), care deservesc sau reprezintă sisteme de control industrial *ICS* (Industrial control systems)/*SCADA* (Supervisory control and data acquisition).

Infrastructurile OT susțin domenii-cheie din energie și industrie, un rol important în securizarea acestora constând în gestionarea riscurilor și vulnerabilităților de securitate cibernetică, precum:

— posibilitatea de accesare în mod neautorizat a echipamentelor/sistemelor de comandă și control din cadrul unor infrastructuri critice;

— afectarea serviciilor de utilitate publică vitale (de exemplu, furnizare energie electrică, energie termică, apă etc.) în urma unor atacuri cibernetice;

— perimarea tehnologiilor utilizate în cadrul infrastructurilor (uzură tehnologică);

— factorul uman care operează infrastructurile.

Din perspectiva securității cibernetice, prezintă relevanță riscurile ce se manifestă la nivelul infrastructurilor OT care sunt, în general, determinate sau conexe unor: deficiențe în monitorizarea acestora sau probleme apărute în depanarea și identificarea anomaliilor (de exemplu, dacă sunt incidente sau configurări greșite ale echipamentelor), probleme ce țin de arhitectura infrastructurii (din teren, cele de control și de proces, din zona de business sau de management etc.), disfuncții pe zona fluxurilor de comunicație, *DMZ* (Demilitarized zone) etc.

Aducerea acestor infrastructuri OT în stare de funcționare în afara parametrilor optimi poate genera un impact considerabil la adresa securității naționale, care se poate traduce în pierderi sau prejudicii economice, afectarea vieții sociale sau chiar pierderea de vieți omenești.

Prin investiția curentă se urmărește creșterea nivelului de securitate cibernetică a entităților publice și private care dețin infrastructuri cu valențe critice, prin:

— evaluarea stării de securitate și a vulnerabilităților rețelelor și sistemelor informatice;

— elaborarea de politici și proceduri de securitate cibernetică în conformitate cu standarde internaționale de securitate a informației și sistemelor informaționale, de management al riscului sau cu cerințele legale aplicabile;

— folosirea soluțiilor care utilizează inteligența artificială;

— asigurarea interoperabilității dintre componentele informatice de securitate;

— protecția sistemelor informatice și a informațiilor vehiculate la nivelul instituțiilor, autorităților publice și operatorilor privați;

— eficientizarea și crearea de premise pentru a continua modernizarea infrastructurilor IT&C cu valențe critice pentru securitatea națională, inclusiv prin minimizarea timpului dedicat activităților de recuperare și restaurare ca urmare a incidentelor sau atacurilor cibernetice.

Implementare

Beneficiarul investiției este Serviciul Român de Informații — Centrul Național Cyberint, prin Unitatea Militară (*U.M.*) 0929 București. Din punct de vedere tehnic, CNC administrează sistemul național de securitate cibernetică, deține resursa umană specializată și know-how-ul în domeniu și va administra infrastructura finanțată prin intermediul proiectului PNRR.

Serviciul Român de Informații (*SRI*), cu statut de instituție publică (conform art. 1 din Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, cu modificările și completările ulterioare), a desemnat U.M. 0929 București pentru planificarea, programarea, coordonarea, asigurarea și controlul componentei de înzestrare a SRI. CNC va fi reprezentat în relația cu celelalte instituții și cu organismele finanțatoare de către U.M. 0929 București pentru implementarea proiectului, în calitate de reprezentant legal.

Descrierea investiției

Investiția va cuprinde următoarele componente:

I. Infrastructura IT și OT aferentă beneficiarilor din categoria IVC

Subcomponente:

— Uniformizarea nivelului de securitate cibernetică pentru IVC-urile incluse în sistemul de securitate dezvoltat prin proiectul SMIS 127221, finanțat și implementat anterior prin Programul operațional Competitivitate 2014-2020

Pentru entitățile incluse în lista beneficiarilor proiectului SMIS 127221 — „Actualizarea și dezvoltarea sistemului național de protecție a infrastructurii IT&C cu valori critice pentru securitatea națională împotriva amenințărilor cibernetice” este necesară asigurarea de upgrade-uri în vederea asigurării aceluiași nivel de protecție cibernetică pentru toate categoriile de beneficiari.

Implementarea proiectului SMIS 127221 a presupus crearea a două categorii de IVC-uri din punctul de vedere al probabilității

cu care acestea pot fi vizate de atacuri cibernetice de tip *APT* (agresiuni cibernetice statale de tip Advanced Persistent Threat), respectiv al impactului pe care un astfel de atac l-ar avea asupra infrastructurii și implicit asupra securității naționale și a statului român. Astfel, infrastructurile/entitățile au fost împărțite în 2 categorii cu grade diferite de asigurare a securității cibernetice (motivat de constrângeri bugetare). Entitățile din categoria a 2-a vor beneficia de upgrade-uri în cadrul proiectului PNRR, cu scopul atingerii aceluiași nivel de securitate cibernetică.

— **Integrarea în sistemul de securitate cibernetică a minimum 42 de IVC-uri noi, cu asigurarea unui nivel de protecție similar**

Minimum 42 de instituții/entități noi vor fi incluse în categoria IVC și infrastructurile aparținând acestora vor fi dotate cu soluții și tehnologii cu rezultate similare din punctul de vedere al nivelului de protecție cibernetică, precum în proiectul dezvoltat anterior — SMIS 127221, astfel încât toți beneficiarii finali vor avea un nivel de securitate cibernetică unitar.

— **Implementarea în cadrul IVC-urilor de tehnologii avansate de protecție cibernetică, ce utilizează un spectru complex de măsuri ce permit identificarea amenințărilor cibernetice, inclusiv a celor ce nu sunt detectate prin echipamentele convenționale de securitate**, cu operaționalizarea cel puțin a următoarelor capabilități:

• sistem avansat de detectare a vulnerabilităților în sistemele informatice și echipamentele de comunicații;

• sistem integrat de identificare a *TTP*-urilor (Tactics, Techniques and Procedures/Tactici, Tehnici și Proceduri) asociate atacurilor cibernetice asupra rețelelor și sistemelor informatice;

• platforma complexă de securitate pentru analiza și procesarea automată a incidentelor cibernetice.

— **Implementarea de soluții de protecție dedicate rețelelor de producție — tip OT (infrastructuri de tip control industrial ICS/SCADA) pentru minimum 9 IVC-uri**, conform specificului activității și infrastructurii operate.

II. Pentru atingerea obiectivelor investiției este necesară **dezvoltarea infrastructurii de securitate cibernetică a CNC**, cu soluții de securitate cibernetică acoperind infrastructuri de tip IT (rețea de business) și OT (rețea de producție — sisteme de control industrial ICS/SCADA).

Prin investiția propusă se vor dezvolta următoarele capabilități:

— sporirea capacității de investigare a CNC (soluții software și hardware);

— platformă pentru securitatea și canalizarea datelor care urmează să fie transferate între rețele cu niveluri de încredere diferite.

III. Complementar activităților pentru dezvoltarea infrastructurii de securitate, proiectul propune și dezvoltarea cunoștințelor în domenii asociate securității cibernetice.

În acest sens, se vor desfășura activități de instruire a personalului unităților partenere și entităților beneficiare în domenii asociate securității cibernetice și altele, fiind avut în vedere un număr minim de 350 de persoane.

Grup-țintă

Grupul-țintă va include 101 instituții și entități (beneficiari indirecți), care au infrastructuri IT&C de importanță critică pentru securitatea națională (categoria IVC). Aceste entități vor include instituții din arcul guvernamental (ministere, agenții, autorități etc.), precum și entități din domeniul energetic (de exemplu, furnizori/distribuitori de gaze, curent electric), domeniul serviciilor esențiale, domeniul sănătății, domeniul transporturilor (de exemplu, aeroporturi, porturi) și domeniul alimentării cu apă și canalizării etc.

Entitățile vizate de proiect se împart în două categorii, astfel:

— entitățile incluse în lista beneficiarilor proiectului implementat anterior „Actualizarea și dezvoltarea sistemului național de protecție a infrastructurii IT&C cu valori critice pentru securitatea națională împotriva amenințărilor cibernetice” (codul SMIS 127221), fiind necesară asigurarea de upgrade-uri;

— entități/infrastructuri noi care vor fi dotate cu soluții și tehnologii cu rezultate similare din punctul de vedere al nivelului de protecție cibernetică ca în proiectul anterior menționat.

— mii lei (inclusiv TVA) —

Valoarea totală a cheltuielilor de investiții (cursul de schimb InforEuro din luna octombrie 2022, respectiv 1 euro = 4,9481 RON)	SRI
	810.936
Eșalonarea cheltuielilor pe ani de implementare	
anul I	447
anul II	720
anul III	0
anul IV	809.769

Conform anexei la Decizia de punere în aplicare a Consiliului (CID) de aprobare a evaluării Planului de Redresare și Reziliență al României 2021/0309 și aranjamentelor operaționale dintre Comisia Europeană și România din 25.05.2022, țintele și jaloanele care trebuie atinse în cadrul acestui contract de finanțare sunt următoarele:

— 179: Entități cu infrastructuri TIC securizate; obiectiv: 101 entități; termen: trimestrul II/2026;

— 179.1: Selectarea entităților publice și private având infrastructuri TIC cu valoare critică pentru securitatea națională; termen: trimestrul IV/2022;

— 179.2: Finalizarea parțială a elementelor de securitate cibernetică pentru entitățile selectate (raport intermediar); termen: trimestrul I/2024;

— 180: Consolidarea centrelor naționale de securitate cibernetică; termen: trimestrul II/2026;

— 180.1: Finalizarea parțială a dezvoltării capacității de protecție integrată a securității infrastructurilor informatice TIC și OT (raport intermediar); termen: trimestrul III/2024.

Durata de execuție a proiectului de investiții: 43 de luni.

Finanțarea investiției

Finanțarea proiectului se realizează din fonduri externe nerambursabile, în cadrul Planului Național de Redresare și Reziliență, componenta 7 — Transformare digitală, investiția 12 — Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente, precum și de la bugetul de stat, prin bugetul Serviciului Român de Informații, în limita sumelor aprobate cu această destinație, conform programelor de investiții publice aprobate potrivit legii.