NOTĂ DE FUNDAMENTARE

Secțiunea 1

Titlul proiectului

HOTĂRÂRE

pentru aprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*”

Secțiunea a 2-a

Motivul emiterii

2.1. Sursa proiectului

Prezentul proiect a fost elaborat la inițiativa Ministerului Afacerilor Interne prin Direcția Generală de Protecție Internă, în baza prevederilor Ordonanței de urgență de Guvernului nr. 30/2007 *privind organizarea și funcționarea Ministerului Afacerilor Interne,* în scopul aprobării Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului „*Sistem de alertă timpurie – SAT (Early warning system)*”.

2.2. Descrierea situației actuale

În contextul derulării proiectului pentru operaționalizarea emiterii cărții electronice de identitate la nivelul Direcției Generale pentru Evidența Persoanelor, la nivelul Ministerului Afacerilor Interne s-a semnat Contractul de finanțare nr. 18441 din 29.08.2024 pentru proiectul de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*“, în cadrul Planului Național de Redresare și Reziliență, Componenta 7 - Transformare digitală, investiția 8 - Cartea de identitate electronică și semnătura digitală calificată, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, Ministerul Afacerilor Interne prin Direcția Generală de Protecție Internă având calitatea de beneficiar.

Implementarea proiectului privind adoptarea CEI, respectiv digitalizarea serviciilor publice ale MAI accesibile prin utilizarea CEI, pentru autentificarea identității în spațiul online, incumbă în mod obligatoriu responsabilitatea asigurării unor condiții adecvate de securitate tehnică și non-tehnică tuturor componentelor, pornind de la facilitățile de producție și managementul post-emitere al CEI până la protejarea resurselor informatice care susțin serviciile digitale împotriva amenințărilor hibride din ce în ce mai complexe, determinate de evoluția accelerată a tehnologiilor emergente/disruptive. Aceste servicii publice electronice au la bază o infrastructura IT&C, compusă din sisteme informatice și de comunicații complexe, larg răspândite pe întregul teritoriu național, inclusiv la nivelul autorităților locale. Prin intermediul infrastructurii respective sunt oferite servicii informaționale atât personalului MAI, cât mai ales populației, existând riscul afectării grave a funcționalității din cauza atacurilor cibernetice executate de către grupările specializate în criminalitate informatică.

În acest sens, perpetuarea și rata crescută de materializare în acțiuni ostile a riscurilor și amenințărilor cibernetice determină mutații semnificative la nivel securitar, fapt pentru care

este necesară adoptarea unei viziuni unitare de răspuns, asumată la nivelul tuturor actorilor implicați în asigurarea securității informatice. Pornind de la nevoia de actualizare permanentă a soluțiilor de securitate cibernetică, implementarea proiectului urmărește o abordare integrată și proactivă în scopul prevenirii, descurajării și contracarării agresiunilor cibernetice complexe.

O abordare integrată performanță-securitate, prin asumarea conceptului „security by design" în limita unor standarde obligatorii, va asigura un grad ridicat de încredere cu impact direct asupra creșterii nivelului de atractivitate a utilizării CEI pentru accesarea serviciilor electronice furnizate de către MAI. În acest sens, se impune operaționalizarea unui Sistem de Alertă Timpurie necesar pentru securizarea rețelelor și sistemelor informatice aferente emiterii CEI și a certificatelor de semnătură electronică avansată, precum și pentru asigurarea unui nivel ridicat de încredere a autentificării în scopul accesării serviciilor publice electronice ale MAI.

În conformitate cu prevederile art. 10 lit. b) din OUG nr. 76/2016, Direcția Generală de Protecție Internă asigură coordonarea și controlul activităților pentru protecția informațiilor clasificate naționale, ale Organizației Tratatului Atlanticului de Nord și ale Uniunii Europene, precum și pentru securitatea cibernetică, la nivelul structurilor Ministerului Afacerilor Interne.

Obiectivul investiției propuse de către DGPI vizează asigurarea unui nivel ridicat de încredere și siguranță pentru creșterea atractivității utilizării CEI și accesării serviciilor electronice publice.

Sistemul reprezintă soluția de securitate optimă pentru asigurarea exploatării sistemelor utilizate în emiterea și punerea in circulație a CEI, precum și pentru utilizarea în mod neîntrerupt și în condiții de siguranță a serviciilor publice electronice furnizate de MAI. În acest fel, se vor crea premisele realizării în mod automat a colectării, procesării, validării și evaluării integrate a datelor și informațiilor multisursă pentru a anticipa, detecta, preveni și contracara amenințările și riscurile de securitate asociate cu emiterea și utilizarea CEI.

În acest context, proiectul SAT reprezintă soluția de securitate pentru asigurarea exploatării în mod neîntrerupt și în condiții de siguranță a sistemelor utilizate în emiterea și punerea în circulație a CEI, precum și consumarea serviciilor publice electronice, motiv pentru care este necesară implementate următoarele activități:

1) Activitatea 1.1 - *Componenta 1* - automatizarea proceselor de colectare, validare și evaluare integrată a datelor și informațiilor multisursă necesare detecției și anticipării amenințărilor de securitate generate de tehnologiile emergente pe baza evaluărilor predictive complexe asociate emiterii și utilizării CEI pentru accesarea serviciilor publice electronice de către populație.

Digitalizarea insuficientă a activității de gestionare a datelor și informațiilor reprezintă principala vulnerabilitate care afectează automatizarea proceselor analitice ale volumelor din ce în ce mai mari de date generate de utilizarea noilor tehnologii și volatilitatea spațiului cibernetic.

Implementarea soluțiilor de tip big data, business intelligence bazate pe inteligența artificială și Machine Learning pentru corelarea automată a unor categorii de date multisursă în scopul consolidării cunoașterii și extinderii capacității de detecție a amenințărilor și riscurilor de

securitate în timp real, impune o etapă pregătitoare. Aceasta vizează implementarea unui concept de tip People-Machine-Systems pentru îmbunătățirea nivelului de digitalizare a capabilităților de colectare și management ale seturilor de date și informații operative, precum și simplificarea integrării lor în instrumente de evaluare/valorificare eficientă în relația cu emitentul CEI și furnizorii interni ai MAI de servicii publice electronice. Nu în ultimul rând, raportându-ne strict la această etapă preliminară, soluțiile înglobează de asemenea tehnologii emergente și conferă un grad crescut de mobilitate.

2) Activitatea 1.2 - *Componenta 2* - extinderea sistemului de securitate și apărare cibernetică al MAI prin dezvoltarea unor capacități tehnice de detecție, monitorizare și analiză a evenimentelor de securitate, interoperabile cu CERT-INT în vederea corelării alertelor cu amenințările cibernetice și optimizarea acțiunilor de anticipare, prevenție și răspuns imediat în cazul apariției unor incidente cibernetice.

În prezent, la nivelul structurilor MAI implicate în fluxurile de preluare a datelor de identitate, personalizare, emitere, activare și de management post-emitere ale CEI nu există capabilități adecvate care să asigure un nivel corespunzător de securitate cibernetică.

De asemenea, pentru cele 11 servicii publice ale MAI ce vor fi digitalizate de către DGCTI conform Jalonului 174 din PNRR, se impune calibrarea senzorilor și capacităților de monitorizare și integrare aferente CERT-INT și centrelor operaționale de securitate sectorială - COSS (existente la nivelul Aparatului Central și principalelor arme).

În acest sens, asigurarea unui nivel crescut de securitate cibernetică necesită identificarea cât mai rapidă a vulnerabilităților infrastructurilor cibernetice aflate în dezvoltare, în raport cu tehnicile actuale utilizate de atacatori, fapt care implică operaționalizarea unui/unor noi COSS, în funcție de rezultatul analizei de risc privind noile infrastructuri informatice asociate CEI și serviciilor publice electronice sus-menționate.

3) Activitatea 1.3 - *Componenta 3* - Back-up și disaster recovery.

Soluția de redundanță și recuperare în caz de dezastru vizează realizarea unei infrastructuri integrate hardware și software care să asigure migrarea/replicarea/stocarea datelor în format electronic în scopul asigurării unei înalte disponibilități necesară menținerii operativității instituționale în situații deosebite, inclusiv în caz de dezastru/calamitate, pentru îndeplinirea funcției de asigurare optimă a suportului privind serviciile electronice.

Sistemul de back-up și disaster recovery acoperă inclusiv infrastructura necesară asigurării redundanței și rezilienței atât din punct de vedere energetic, cât și în ceea ce privește securitatea cibernetică.

Implementarea soluției va ține cont de cerințele specifice privind amplasarea într-o zonă suficient de departe din punct de vedere geografic față de București pentru asigurarea funcționării sistemului în cazul unui posibil dezastru, fiind luat în calcul inclusiv caracterul de mobilitate al acesteia.

2.3. Schimbări preconizate

Proiectul DGPI va contribui la consolidarea nivelului de securitate cibernetică și extinderea soluțiilor de securitate inclusiv prin crearea și extinderea unor centre de securitate operaționale

dedicate infrastructurii IT&C existentă la nivelul MAI pentru emiterea, managementul post-emitere al CEI și furnizarea celor 11 servicii publice electronice, facilitând interacțiunea digitală dintre entitățile publice/private și cetățeni, prin intermediul unei infrastructuri informatice sigure și reziliente.

Prin realizarea acestui sistem, beneficiarul abordează provocările de securitate asociate celor 11 servicii publice electronice furnizate populației de către MAI, infrastructurii IT&C utilizată pentru emiterea și managementul post-emitere a CEI, precum și proceselor de autentificare/accesare a acestora de către utilizatorii persoane fizice sau juridice.

2.4. Alte informații

Valoarea totală a investiției prevăzute în anexa nr. 1 este de 106.421 mii lei, inclusiv TVA. În conformitate cu prevederile art. 42 alin. (1) lit. a) din Legea nr. 500/2002 *privind finanțele publice*, cu modificările și completările ulterioare, este necesară aprobarea Guvernului pentru nota de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente categoriilor de investiții incluse la poziția C „*Alte cheltuieli de investiții*" din programele de investiții publice și a căror valoare depășește 100 milioane lei.

În cadrul Planului Național de Redresare și Reziliență, Componenta 7 – Transformare digitală, Investiția 8 – Cartea de identitate electronică și semnătura digitală, Jalonul 174, a fost aprobat și proiectul „*D4eID – Digitalizare pentru promovarea cărții de identitate electronice*", implementat de către Direcția Generală pentru Comunicații și Tehnologia Informației și Direcția Informare și Relații Publice, proiectul „*Sistem de alertă timpurie – SAT (Early warning system)*" fiind complementar acestuia.

Nota de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*D4eID – Digitalizare pentru promovarea cărții de identitate electronice*" a fost aprobată prin Hotărârea de Guvern nr. 1407 din 14 noiembrie 2024.

Secțiunea a 3-a

Impactul socioeconomic

3.1. Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ

3.2. Impactul social

Proiectul propus contribuie la măsurile de sprijin finanțate pentru implementarea CEI prin crearea unei infrastructuri cu nivel ridicat de încredere și siguranță, necesară atât emiterii, punerii în circulație și asigurării funcționalității și disponibilității CEI, cât și a serviciilor accesate prin intermediul acesteia.

Astfel, va fi implementat un sistem care să adreseze riscurile de securitate (tehnice și non tehnice), creând premisele facilitării interacțiunii digitale dintre entitățile publice/private și cetățeni. Acesta vine în completarea celorlalte două măsuri de sprijin (11 servicii publice online, cu un nivel de sofisticare de cel puțin „3", respectiv o campanie de sensibilizare care să încurajeze utilizarea pe scară largă a cărții de identitate electronice și, implicit, a serviciilor publice electronice aferente acesteia) contribuind, astfel, la creșterea atractivității și utilizării CEI pe scară largă, în rândul populației.

3.3. Impactul asupra drepturilor și libertăților fundamentale ale omului
3.4. Impactul macroeconomic
3.4.1. Impactul asupra economiei și asupra principalilor indicatori macroeconomici
3.4.2. Impactul asupra mediului concurențial și domeniul ajutoarelor de stat
3.5. Impactul asupra mediului de afaceri
3.6. Impactul asupra mediului înconjurător
3.7. Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării
3.8. Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile
3.9. Alte informații

Secțiunea a 4-a

Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani), inclusiv informații cu privire la cheltuieli și venituri

- mii lei -

Indicatori	Anul curent	Următorii patru ani				Media pe 5 ani
1	2025	2026	2027	2028	2029	
4.1. Modificări ale veniturilor bugetare, plus/minus, din care:	-	-	-	-	-	-
a) buget de stat, din acesta: (i) impozit pe profit (ii) impozit pe venit	-	-	-	-	-	-
b) bugete locale: (i) impozit pe profit	-	-	-	-	-	-
c) bugetul asigurărilor sociale de stat: (i) contribuții de asigurări d) alte tipuri de venituri	-	-	-	-	-	-
4.2. Modificări ale cheltuielilor bugetare, plus / minus, din care:	-	-	-	-	-	-

a) buget de stat, din acesta: (i) cheltuieli de personal (ii) bunuri și servicii	-	-	-	-	-	-
b) bugete locale: (i) cheltuieli de personal (ii) bunuri și servicii	-	-	-	-	-	-
c) bugetul asigurărilor sociale de stat: (i) cheltuieli de personal (ii) bunuri și servicii	-	-	-	-	-	-
d) alte tipuri de cheltuieli	-	-	-	-	-	-
4.3. Impact financiar, plus/minus, din care: a) buget de stat b) bugete locale	-	-	-	-	-	-
4.4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
4.5. Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6. Calcule detaliate privind fundamentarea modificărilor veniturilor și / sau cheltuielilor bugetare						

4.7. Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: a) fișa financiară prevăzută la art. 15 din Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată; b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele și prioritățile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală și cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară**.**
4.8. Alte informații Finanțarea proiectului de investiții prevăzut în anexa nr. 1 se realizează din fonduri externe nerambursabile, în cadrul Planului național de redresare și reziliență, Componenta 7 - Transformare digitală, Investiția 8 - Cartea de identitate electronică și semnătura digitală, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, și de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.. Referitor la *documentul de avizare a principalelor caracteristici ale proiectului de investiții, aprobat de către ordonatorul principal de credite*, menționăm că acesta are caracter clasificat secret de serviciu, fiind înregistrat cu nr. S/2135307 din 12.07.2024. Mai mult, raportat la caracteristicile proiectului de investiții, precizăm că acestea se regăsesc în cererea de finanțare ce reprezintă anexă la contractul de finanțare semnat de către ordonatorul principal de credite. În privința menționării valorii anuale a investiției, pentru fiecare an de finanțare, inclusiv pentru anul I, având în vedere că durata de execuție a proiectului este eșalonată pentru perioada de 22 de luni, precizăm că, din cadrul secțiunii *Planul achizițiilor* din Cererea de finanțare transmisă, reiese faptul că în primul an de finanțare (august 2024-august 2025) nu vor exista cheltuieli de investiții, primele angajamente legale urmând să fie încheiate după luna iulie 2025.

Secțiunea a 5-a

Efectele proiectului asupra legislației în vigoare

5.1. Măsuri normative necesare pentru aplicarea prevederilor prezentului proiect
5.2. Impactul asupra legislației în domeniul achizițiilor publice
5.3. Conformitatea proiectului cu legislația UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE).
5.3.1. Măsuri normative necesare transpunerii directivelor UE
5.3.2. Măsuri normative necesare aplicării actelor legislative ale UE
5.4. Hotărâri ale Curții de Justiție a Uniunii Europene
5.5. Alte acte normative și/sau documente internaționale din care decurg angajamente asumate
5.6. Alte informații

Secțiunea a 6-a

Consultările efectuate în vederea elaborării proiectului

6.1. Informații privind neaplicarea procedurii de participare la elaborarea actelor normative
6.2. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate
6.3. Informații despre consultările organizate cu autoritățile administrației publice locale
6.4. Informații privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative
6.5. Informații privind avizarea de către: **a) Consiliul Legislativ** **b) Consiliul Suprem de Apărare a Țării** **c) Consiliul Economic și Social** **d) Consiliul Concurenței** **e) Curtea de Conturi**
6.6. Alte informații

Secțiunea a 7-a

Activități de informare publică privind elaborarea și implementarea proiectului

7.1. Informarea societății civile cu privire la necesitatea elaborării proiectului Proiectul are caracter individual, sens în care nu sunt incidente dispozițiile Legii nr. 52/2003 privind transparența decizională în administrația publică, cu modificările și completările ulterioare.
7.2. Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării actului normativ, precum și efectele asupra sănătății și securității cetățenilor sau diversității biologice

Secțiunea a 8-a

Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ

8.1. Măsurile de punere în aplicare a proiectului de act normativ
8.2. Alte informații

Față de cele prezentate, a fost elaborat **proiectul de hotărâre a Guvernului pentru aprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*”,** pe care îl supunem spre adoptare Guvernului.

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE

Marian-Cătălin PREDOIU

AVIZAT:

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE

Marcel-Ioan BOLOȘ

VICEPRIM-MINISTRU,
MINISTRUL FINANȚELOR

TÁNCZOS Barna

GUVERNUL ROMÂNIEI

HOTĂRÂRE
pentru aprobarea Notei de fundamentare privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*”

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 aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*” din cadrul Componentei 7 - Transformare digitală din Planul național de redresare și reziliență, prevăzută în anexa care face parte integrantă din prezenta hotărâre.

Art. 2 - Finanțarea proiectului de investiții prevăzut la art. 1 se realizează din fonduri externe nerambursabile, în cadrul Planului național de redresare și reziliență, Componenta 7 - Transformare digitală, Investiția 8 - Cartea de identitate electronică și semnătura digitală, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, și de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.

Art. 3 - Ministerul Afacerilor Interne, prin Direcția Generală de Protecție Internă, răspunde de modul de utilizare a sumelor prevăzute în anexa nr. 1, în conformitate cu prevederile legale în vigoare.

PRIM-MINISTRU

ION-MARCEL CIOLACU

anexa

NOTĂ DE FUNDAMENTARE

privind necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*”

Potrivit art. 1 din Ordonanța de urgență a Guvernului nr. 76/2016 *privind înființarea, organizarea și funcționarea Direcției Generale de Protecție Internă a Ministerului Afacerilor Interne,* Direcția Generală de Protecție Internă este structura specializată cu atribuții în domeniul securității naționale, în subordinea Ministerului Afacerilor Interne, cu personalitate juridică, care desfășoară activități de identificare, contracarare și înlăturare a amenințărilor, vulnerabilităților și factorilor de risc la adresa informațiilor, patrimoniului, personalului, misiunilor, procesului decizional și capacității operaționale ale structurilor Ministerului Afacerilor Interne, precum și a celor care pot duce la tulburarea gravă a ordinii publice.

Totodată, în conformitate cu prevederile art. 10 lit. b) din același act normativ, Direcția Generală de Protecție Internă asigură coordonarea și controlul activităților pentru protecția informațiilor clasificate naționale, ale Organizației Tratatului Atlanticului de Nord și ale Uniunii Europene, precum și pentru securitatea cibernetică, la nivelul structurilor Ministerului Afacerilor Interne.

Implementarea proiectului privind adoptarea CEI, respectiv digitalizarea serviciilor publice ale MAI accesibile prin utilizarea CEI, pentru autentificarea identității în spațiul online, incumbă în mod obligatoriu responsabilitatea asigurării unor condiții adecvate de securitate tehnică și non-tehnică tuturor componentelor, pornind de la facilitățile de producție și managementul post-emitere al CEI până la protejarea resurselor informatice care susțin serviciile digitale împotriva amenințărilor hibride din ce în ce mai complexe, determinate de evoluția accelerată a tehnologiilor emergente/disruptive. Aceste servicii publice electronice au la bază o infrastructura IT&C, compusă din sisteme informatice și de comunicații complexe, larg răspândite pe întregul teritoriu național, inclusiv la nivelul autorităților locale. Prin intermediul infrastructurii respective sunt oferite servicii informaționale atât personalului MAI, cât mai ales populației, existând riscul afectării grave a funcționalității din cauza atacurilor cibernetice executate de către grupările specializate în criminalitate informatică.

În acest sens, perpetuarea și rata crescută de materializare în acțiuni ostile a riscurilor și amenințărilor cibernetice determină mutații semnificative la nivel de securitate, fapt pentru care este necesară adoptarea unei viziuni unitare de răspuns, asumată la nivelul tuturor entităților implicate în asigurarea securității informatice. Pornind de la nevoia de actualizare permanentă a soluțiilor de securitate cibernetică, implementarea proiectului urmărește o abordare integrată și proactivă în scopul prevenirii, descurajării și contracarării agresiunilor cibernetice complexe.

O abordare integrată performanță-securitate, prin asumarea conceptului „*security by design*” în limita unor standarde obligatorii, va asigura un grad ridicat de încredere cu impact direct asupra creșterii nivelului de atractivitate a utilizării CEI pentru accesarea serviciilor electronice furnizate de către MAI. În acest sens, se impune operaționalizarea unui Sistem de Alertă Timpurie necesar pentru securizarea rețelelor și sistemelor informatice aferente emiterii CEI și a certificatelor de semnătură electronică avansată, precum și pentru asigurarea unui nivel ridicat de încredere a autentificării în scopul accesării serviciilor publice electronice ale MAI.

La nivelul Ministerului Afacerilor Interne s-a semnat Contractul de finanțare nr. 18441 din 29.08.2024 pentru proiectul de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*“, în cadrul Planului Național de Redresare și Reziliență, Componenta 7 - Transformare digitală, Investiția 8 - Cartea de identitate electronică și semnătura digitală calificată, Jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, având calitatea de beneficiar Ministerul Afacerilor Interne, prin Direcția Generală de Protecție Internă.

Obiectivul investiției propuse de către DGPI vizează asigurarea unui nivel ridicat de încredere și siguranță pentru creșterea atractivității utilizării CEI și accesării serviciilor electronice publice.

Sistemul reprezintă soluția de securitate optimă pentru asigurarea exploatării sistemelor utilizate în emiterea și punerea in circulație a CEI, precum și pentru utilizarea în mod neîntrerupt și în condiții de siguranță a serviciilor publice electronice furnizate de MAI. În acest fel, se vor crea premisele realizării în mod automat a colectării, procesării, validării și evaluării integrate a datelor și informațiilor multisursă pentru a anticipa, detecta, preveni și contracara amenințările și riscurile de securitate asociate cu emiterea și utilizarea CEI.

În acest context, proiectul SAT reprezintă soluția de securitate pentru asigurarea exploatării în mod neîntrerupt și în condiții de siguranță a sistemelor utilizate în emiterea și punerea în circulație a CEI, precum și consumarea serviciilor publice electronice, motiv pentru care este necesară implementate următoarele activități:

1) Activitatea 1.1 - *Componenta 1* - automatizarea proceselor de colectare, validare și evaluare integrată a datelor și informațiilor multisursă necesare detecției și anticipării amenințărilor de securitate generate de tehnologiile emergente pe baza evaluărilor predictive complexe asociate emiterii și utilizării CEI pentru accesarea serviciilor publice electronice de către populație.

Digitalizarea insuficientă a activității de gestionare a datelor și informațiilor reprezintă principala vulnerabilitate care afectează automatizarea proceselor analitice ale volumelor din ce în ce mai mari de date generate de utilizarea noilor tehnologii și volatilitatea spațiului cibernetic.

Implementarea soluțiilor de tip big data, business intelligence bazate pe inteligența artificială și Machine Learning pentru corelarea automată a unor categorii de date multisursă în scopul consolidării cunoașterii și extinderii capacității de detecție a amenințărilor și riscurilor de securitate în timp real, impune o etapă pregătitoare. Aceasta vizează implementarea unui concept de tip People-Machine-Systems pentru îmbunătățirea nivelului de digitalizare a capabilităților de colectare și management ale seturilor de date și informații operative, precum și simplificarea integrării lor în instrumente de evaluare/valorificare eficientă în relația cu emitentul CEI și furnizorii interni ai MAI de servicii publice electronice. Nu în ultimul rând, raportându-ne strict la această etapă preliminară, soluțiile înglobează de asemenea tehnologii emergente și conferă un grad crescut de mobilitate.

2) Activitatea 1.2 - *Componenta 2* - extinderea sistemului de securitate și apărare cibernetică al MAI prin dezvoltarea unor capacități tehnice de detecție, monitorizare și analiză a evenimentelor de securitate, interoperabile cu CERT-INT în vederea corelării alertelor cu amenințările cibernetice și optimizarea acțiunilor de anticipare, prevenție și răspuns imediat în cazul apariției unor incidente cibernetice.

În prezent, la nivelul structurilor MAI implicate în fluxurile de preluare a datelor de identitate, personalizare, emitere, activare și de management post-emitere ale CEI nu există capabilități adecvate care să asigure un nivel corespunzător de securitate cibernetică.

De asemenea, pentru cele 11 servicii publice ale MAI ce vor fi digitalizate de către DGCTI conform Jalonului 174 din PNRR, se impune calibrarea senzorilor și capacităților de monitorizare și integrare aferente CERT-INT și centrelor operaționale de securitate sectorială - COSS (existente la nivelul Aparatului Central și principalelor arme).

În acest sens, asigurarea unui nivel crescut de securitate cibernetică necesită identificarea cât mai rapidă a vulnerabilităților infrastructurilor cibernetice aflate în dezvoltare, în raport cu tehnicile actuale utilizate de atacatori, fapt care implică operaționalizarea unui/unor noi COSS, în funcție de rezultatul analizei de risc privind noile infrastructuri informatice asociate CEI și serviciilor publice electronice sus-menționate.

3) **Activitatea 1.3 - *Componenta 3*** - Back-up și disaster recovery.

Soluția de redundanță și recuperare în caz de dezastru vizează realizarea unei infrastructuri integrate hardware și software care să asigure migrarea/replicarea/stocarea datelor în format electronic în scopul asigurării unei înalte disponibilități necesară menținerii operativității instituționale în situații deosebite, inclusiv în caz de dezastru/calamitate, pentru îndeplinirea funcției de asigurare optimă a suportului privind serviciile electronice.

Sistemul de back-up și disaster recovery acoperă inclusiv infrastructura necesară asigurării redundanței și rezilienței atât din punct de vedere energetic, cât și în ceea ce privește securitatea cibernetică.

Implementarea soluției va ține cont de cerințele specifice privind amplasarea într-o zonă suficient de departe din punct de vedere geografic față de București pentru asigurarea funcționării sistemului în cazul unui posibil dezastru, fiind luat în calcul inclusiv caracterul de mobilitate al acesteia.

Proiectul propus contribuie la măsurile de sprijin finanțate pentru implementarea CEI prin crearea unei infrastructuri cu nivel ridicat de încredere și siguranță, necesară atât emiterii, punerii în circulație și asigurării funcționalității și disponibilității CEI, cât și a serviciilor accesate prin intermediul acesteia.

Astfel, va fi implementat un sistem care să adreseze riscurile de securitate (tehnice și non tehnice), creând premisele facilitării interacțiunii digitale dintre entitățile publice/private și cetățeni. Acesta vine în completarea celorlalte două măsuri de sprijin (11 servicii publice online, cu un nivel de sofisticare de cel puțin „3”, respectiv o campanie de sensibilizare care să încurajeze utilizarea pe scară largă a cărții de identitate electronice și, implicit, a serviciilor publice electronice aferente acesteia) contribuind, astfel, la creșterea atractivității și utilizării CEI pe scară largă, în rândul populației.

Prin implementarea SAT, minim 10.000 de cetățenii vor beneficia anual de CEI și de servicii publice online sigure, cu grad înalt de disponibilitate și reziliență, fiind create premisele dezvoltării capabilităților tehnologice și implicit a infrastructurii IT&C prin implementarea unor soluții de nouă generație, interconectate, care să permită conjugarea eforturilor structurilor MAI în scopul prestării serviciilor publice digitale la un nivel ridicat de securitate, față de riscurile din ce în ce mai diversificate pe fondul evoluției rapide a tehnologiilor emergente.

Proiectul DGPI va contribui la securizarea infrastructurii IT&C existentă la nivelul MAI pentru emiterea, managementul post-emitere al CEI și furnizarea celor 11 servicii publice

electronice, facilitând interacțiunea digitală dintre entitățile publice/private și cetățeni, prin intermediul unei infrastructuri informatice sigure și reziliente.

Prin realizarea acestui sistem, beneficiarul abordează provocările de securitate asociate celor 11 servicii publice electronice furnizate populației de către MAI, infrastructurii IT&C utilizată pentru emiterea și managementul post-emitere a CEI, precum și proceselor de autentificare/accesare a acestora de către utilizatorii persoane fizice sau juridice.

Valoarea totală a proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*“ pentru care s-a semnat Contractul de finanțare nr. 18441 din 29.08.2024 este în sumă de 106.421 mii lei (inclusiv TVA).

Caracteristicile principale și indicatorii tehnico-economici aferenți proiectului de investiții „*Sistem de alertă timpurie – SAT (Early warning system)*“

Titular: Ministerul Afacerilor Interne

Beneficiar: Direcția Generală de Protecție Internă

Amplasament: sediile Ministerului Afacerilor Interne - Direcția Generală de Protecție Internă.

Indicatori tehnico-economici

Valoarea totală a cheltuielilor de investiții (inclusiv TVA) (în prețuri valabile în luna martie 2024: 1 euro = 4,9683 lei)	**mii lei**	**106.421**
Eșalonarea investiției		
- Anul I	**mii lei**	**-**
- Anul II	**mii lei**	**106.421**
Activitatea 1.1 - *Componenta 1* - automatizarea proceselor de colectare, validare și evaluare integrată a datelor și informațiilor multisursă necesare detecției și anticipării amenințărilor de securitate generate de tehnologiile emergente pe baza evaluărilor predictive complexe asociate emiterii și utilizării CEI pentru accesarea serviciilor publice electronice de către populație.	**cpl.**	**1**
Activitatea 1.2 - *Componenta 2* - extinderea sistemului de securitate și apărare cibernetică al MAI prin dezvoltarea unor capacități tehnice de detecție, monitorizare și analiză a evenimentelor de securitate, interoperabile cu CERT-INT în vederea corelării alertelor cu amenințările cibernetice și optimizarea acțiunilor de anticipare, prevenție și răspuns imediat în cazul apariției unor incidente cibernetice.	**cpl.**	**1**
Activitatea 1.3 - *Componenta 3* - Back-up și disaster recovery pentru sistemul de alertă timpurie cu privire la riscurile de securitate (inclusiv riscurile cibernetice) asociate CEI și serviciilor publice electronice ale MAI.	**cpl.**	**1**
Durata de execuție a proiectului (dar nu mai târziu de 30 iunie 2026)	**luni**	**22**

Finanțarea proiectului de investiții se realizează din fonduri externe nerambursabile, în cadrul Planului național de redresare și reziliență, componenta 7 - Transformare digitală,

investiția 8 - Cartea de identitate electronică și semnătura digitală, jalon 174 - Punerea în aplicare a măsurilor de sprijin pentru implementarea cărții de identitate electronice, și de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, în limita sumelor aprobate anual cu această destinație, conform programelor de investiții publice aprobate potrivit legii.