ANUNȚ DE PARTICIPARE

privind achiziționarea: ***Serviciilor de testare securității cibernetice pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT a CNAS anul 2026***

prin procedura de achiziție: *Cererea ofertelor de preț*

***Procedura a fost inclusă în planul de achiziții publice a autorității contractante (Da/Nu): Da**

Link-ul către planul de achiziții publice publicat:
https://cnas.gov.md/ro/transparenta/achizitii-publice/planuri-de-achizitii-publice

1. **Denumirea autorității contractante:** *Casa Națională de Asigurări Sociale*
2. **IDNO:** *1004600030235*
3. **Adresa:** *mun. Chișinău, str. Gh. Tudor,3*
4. **Numărul de telefon/fax:** *022-257-681; 022-257-840*
5. **Adresa de e-mail și de internet a autorității contractante:** achizitiicnas@cnas.gov.md , www.cnas.gov.md
6. **Adresa de e-mail sau pagina web oficială de la care se va putea obține accesul la documentația de atribuire:** *documentația de atribuire este anexată în cadrul procedurii în SIA RSAP* .
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** *Nu se aplică*
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea următoarelor bunuri:**
   ***Codul CPV:* 79417000-0** (Servicii de consultanţă în domeniul securităţii)

Nr.	Specificația tehnică serviciilor	Valoarea estimativă lei fără TVA	Pasul minim, lei
Lotul 1	**Serviciile de testare securității cibernetice pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT a CNAS anul 2026**		
	Cerințe pentru servicii de testare securității cibernetice pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT a CNAS. **1.1. Obiectul achiziției** Obiectul achiziției reprezintă contractarea serviciilor de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități, consultanță, testare a securității cibernetice din cadrul CNAS) care vor include: 1.1.1. Scanarea de vulnerabilități conform standardelor internaționale cu instrumente speciale. Analiza vulnerabilităților sistemelor informaționale CNAS (inclusiv din Cloud) și identificarea celor adevărate din cele false. Raportarea către CNAS a vulnerabilităților depistate și recomandările viabile de fixare. Consultanță la fixarea vulnerabilităților și a breșelor de securitate depistate precum și consultanță la aplicarea măsurilor compensatorii de protecție cibernetică. Prin acest serviciu se va asigura identificarea posibilelor vulnerabilități care apar zilnic la nivelul sistemelor de operare, bazelor de date și aplicațiilor software. 1.1.2. Consultanță în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN, LAN, a elementelor IT, prin analiza eficacității tehnologice a soluțiilor de protecție automatizate, a ecranelor de protecție precum și consultanță la aplicarea cerințelor minime de securitate cibernetică pentru instituțiile de stat. Consultarea continuă conform standardelor internaționale la identificarea anumitor soluții și a produselor necesare securizării sistemului informațional al Autorității contractante.	**350 000,00**	**3 500,00**

	1.1.3. Servicii de teste de penetrare (Penetration testing) a infrastructurii autorității contractante din exteriorul infrastructurii și din interiorul acesteia. Ofertantul va prezenta în Planul de proiect, vectori de atac reali care ar putea fi aplicați de către persoane necunoscute în scopul sustragerii datelor din cadrul sistemelor informaționale sau subminării securității informaționale. 1.1.4. Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute într-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența ca acestea vor fi efectuate într-un mod etic, cu permisiunea Beneficiarului. Procesul implica o analiza activa a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvata și din breșe cunoscute sau necunoscute, hardware și software. 1.1.5. Testarea practică a angajaților prin diverse tehnici de manipulare la disponibilitatea de a oferi date tehnice interne persoanelor terțe - inginerie socială. **1.2. Scopul serviciilor prestate** 1.2.1. Scopul serviciilor enumerate mai sus este asigurarea unui climat funcțional și protejat al sistemului informațional precum și asigurarea cerințelor minime obligatorii de securitate cibernetică pentru instituțiile de stat. 1.2.2. Resursele care sunt expuse testelor de penetrare sunt: • 43 IP adrese externe, oficiile teritoriale. • 7 aplicații web. • Subrețele interne. 1.2.3. Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe. Ofertantul trebuie să prezinte informație despre modul în care intenționează să presteze serviciile solicitate la nivelul cerut și să le descrie în Planul de proiect. **2.1. Cerințele față de servicii** 2.1.1. Serviciile de scanări de vulnerabilități vor avea ca rezultat o analiză complexă a gradului de pericol a vulnerabilităților și breșelor de securitate din sistemele informatice. Vor fi raportate și examinate de către experții Ofertantului vulnerabilitățile cu pericol sporit de securitate și fiecărei vulnerabilități îi vor fi atribuite recomandări de fixare. Scanarea de vulnerabilități va genera un Raport de vulnerabilități prezentat și explicat în detalii conducerii Autorității contractante. 2.1.2. Consultanță în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN, LAN, a elementelor IT vor asigura o informare continuă despre cele mai noi tehnici și metodologii de securizare precum și analiza de către experții Ofertantului a implementării corecte și setării suficiente a ecranelor de protecție gen firewall la nivel de stații, servere, echipamente de rețea, etc. 2.1.3. Testele de penetrare reprezintă o evaluare complexă a securității sistemelor informatice ale Beneficiarului, testând eficacitatea masurilor de securitate implementate prin simularea unor atacuri informatice. Activitățile echipei de testare se vor baza pe practici de "ethical hacking", iar posturile pe care le va lua echipa va fi mixt alcătuit din următoarele: a. Black box – în această situație, echipa de testare nu deține informații despre sistemele auditate, cu excepția datelor necesare pentru accesarea aplicațiilor (de exemplu: pagini web, adrese IP). Testarea se realizează din perspectiva unui atacator extern, fără cunoștințe interne despre infrastructură sau cod. Această metodă este utilizată în principal pentru evaluarea securității infrastructurii externe a Beneficiarului. b. Grey Box – echipa de experți va cunoaște unele informații ce țin de topologia infrastructurii precum și conturi de acces de utilizator. Testarea din interior a infrastructurii va include minim vectorii de atac în scop de re-evaluare a testului de penetrare precedent. 2.1.4. Ofertantul va trebui sa utilizeze echipamente și aplicații, și să dețină experiența pentru realizarea de teste de penetrare la nivel de rețea, sistem de operare, baze de date, Cloud și aplicații, inclusiv cele web, acțiuni simulate de negare a serviciului (DoS). 2.1.5. Ofertantul va trebui sa dețină și să utilizeze echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice țința, identificarea de vulnerabilități, și formularea unor recomandări de remediere. 2.1.6. Ofertantul va trebui sa dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate in scopul testării.		

2.2. Cerințe față de livrabilele proiectului

Ca urmare a serviciilor prestate, Ofertantul selectat va oferi cel puțin următoarele livrabile:

- Plan de proiect;
- Plan de scanări și testare;
- Planul de acțiuni (SOW - Scope of Work);
- Metodologia și cadru de testare care urmeaza a fi efectuata;
- Raportul de scanări de vulnerabilități care vor include vulnerabilitățile detectate pe parcursul, catalogate în funcție de gravitatea lor. Raportul va include:
  - Descrierea vulnerabilităților;
  - Analiza vulnerabilităților și atribuirea gradelor de pericol;
  - Recomandări și modalități de remediere;
  - Consultanță de fixare a breșelor și vulnerabilităților.
- Rapoarte de analiză, ce vor conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate.

2.3. Testele de penetrare vor include cel puțin:

a. Obținerea informațiilor din domeniul public;
b. Scanarea sistemelor din pct. 1.2.2.;
c. Tehnici de enumerare:

- Identificarea sistemelor de operare;
- Identificarea patch-urilor de securitate lipsă pe un anumit sistem de operare;
- Determinarea vulnerabilităților cunoscute la nivelul sistemelor de operare;
- Identificarea tuturor porturilor deschise;
- Identificarea serviciilor care rulează pe un anumit port;
- Determinarea vulnerabilităților cunoscute la nivelul serverelor de aplicații;
- Determinarea vulnerabilităților cunoscute pentru bazele de date;
- Determinarea vulnerabilităților cunoscute la nivelul serviciilor active identificate;
- Identificarea problemelor de configurare;
- Exploatarea vulnerabilităților identificate.

d. Obținerea accesului neautorizat prin exploatarea vulnerabilităților, respectiv a problemelor de configurație;
e. Consolidarea accesului.

2.4. Metodologia de testare elaborată și folosită de către ofertant va fi în conformitate cu bunele practici internaționale precum: OWASP, OSSTMM, ISSAF, NIST, ISACA etc.

2.5. În realizarea testelor de penetrare, ofertantul va realiza următorii pași:

a. Construirea unui model al amenințărilor. Investigarea arhitecturii infrastructurii și a tehnologiei. Identificarea specificațiilor cheie de securitate și a amenințărilor. Crearea unui model al amenințărilor care documentează activele care trebuie protejate, potențialele amenințări la adresa acestor active, atacurile care ar putea fi realizate, precum și condițiile care ar duce la atacuri de succes.

b. Construirea unui plan de evaluare și acțiune. Convertirea amenințărilor posibile în atacuri care vor fi realizate de ingineri de securitate.

c. Executarea evaluării. Executarea atacurilor, așa cum sunt descrise în planul de acțiune. Descoperirea vulnerabilităților și a variațiilor acestora.

d. Raportarea rezultatelor (trebuie să includă un sumar pentru persoanele care nu sunt experți IT). Documentarea problemelor identificate și prezentarea unor recomandări pentru remediere (trebuie să includă clasificări bazate pe CVE și

CVSS cel puțin V3).

2.6. Cerințe față de testele de penetrare pentru aplicațiile web. Testarea de securitate la nivelul aplicațiilor web este realizată în concordanță cu metodologia OWASP, certificată la nivel mondial. Atacurile din planul de testare vizează în principal următoarele aspecte:

a. Testarea mecanismelor de păstrare a confidențialității și integrității datelor;
b. Testarea procesului de Management al Identității;
c. Testarea mecanismelor de Management al configurațiilor;
d. Testarea mecanismelor de Autentificare;
e. Testarea mecanismelor de Autorizare;
f. Testarea mecanismelor de Management al Sesiunilor;
g. Testarea mecanismelor de Validare a Datelor;
h. Testarea mecanismelor de management al Excepțiilor (erorilor);
i. Testarea mecanismelor Criptografice;

2.7. Cerințe față de descrierea vulnerabilităților identificate. Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice (cel puțin diagrame, grafice sau hărți). Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Raportul va conține cel puțin următoarele capitole:

a. Sumar executiv;
b. Obiectivele și scopul evaluării;
c. Prezentare succintă a metodologiei utilizate în cadrul testării;
d. Descrierea contextului în care s-a desfășurat testarea;
e. Prezentarea individuală a vulnerabilităților descoperite, după cum urmează:

- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere.

f. Alte detalii și recomandări;
g. Anexa cu lista testelor de securitate efectuate.

2.8. Cerințe față de analiza de risc. În vederea realizării acestei analize de risc, se realizează următoarele:
a. Identificarea elementelor analizate: sisteme, aplicații, procese, oameni;
b. Identificarea vulnerabilităților și a amenințărilor;
c. Cuantificarea și măsurarea scenariilor de risc;
d. Identificarea controalelor aplicabile;
e. Stabilirea registrului de riscuri și identificarea riscurilor reziduale sau a scenariilor necontrolate.

2.9. Cerințe față de raportul de prezentare și activitățile ulterioare.

Raportul are ca scop prezentarea concluziilor primare și a analizelor rezultate din datele culese în procesul de testare. În urma finalizării activităților de testare, în cadrul unei ședințe de închidere tip workshop, ofertantul va prezenta concluziile activității de testare și va realiza agrearea cu observațiile beneficiarului testării pe principalele domenii funcționale. De asemenea, în cadrul ședinței va fi prezentat, în formă draft, „Raportul de testare", raport care va fi îmbunătățit pe baza rezultatelor dezbaterilor.

Raportul de testare va include:
a. Limitări privind divulgarea și utilizarea raportului de testare a vulnerabilităților;

b. Introducere (rezumat al serviciilor prestate, aria de acoperire și perioada);
c. Sumar executiv:

- Obiectivele și scopul testului de scanare a vulnerabilităților;
- Descrierea contextului în care s-a desfășurat testul de penetrare;

d. Prezentarea individuală a vulnerabilităților descoperite, după cum urmează:

- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere;
- Alte detalii și recomandări.

e. Identificarea vulnerabilităților precum:

- Generale;
- Clasificate pe categorie;
- Clasificate pe risc;
- Raport al vulnerabilităților în detaliu care va conține: un sumar, scoring-ul de risc, descrierea riscului, descrierea tehnică, remedierea.

f. Anexa cu lista testelor de securitate efectuate.

Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/măsuri/metode care trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de problemele și vulnerabilitățile detectate, precum și recomandări și propuneri de implementare ale acestora.

2.10. După confirmarea remedierii vulnerabilităților identificate de către beneficiar, ofertantul va realiza o testare repetată pentru a confirma închiderea vulnerabilităților identificate.

3.1. Cerinte fată de membrii echipei de proiect ofertată:

Ofertantul (Prestatorul) trebuie să prezinte dovezi că poate pune la dispoziția Beneficiarului pentru executarea contractului de achiziție publică ce face obiectul prezentei achiziții, un număr minim de experți-cheie, după cum urmează:

a. Expert-cheie - Manager de proiect
b. Expert-cheie – Expert 1
- Expert testare securitate infrastructură rețea de diferit tip
- Expert testare securitate cloud (public, privat, hybrid)

c. Expert-cheie – Expert 2
- Expert testare securitate sisteme informatice
- Expert testare securitate aplicații

Ofertantul trebuie sa facă dovada îndeplinirii de către experții cheie a următoarelor criterii:

3.1.1. Expert-cheie nr. 1 - Manager de proiect este responsabil de gestiunea eficientă a proiectului. Experiența în domeniul protecției datelor cu caracter personal constituie un avantaj. Deținător al cetățeniei Republicii Moldova.
a. Experiență de cel puțin 5 ani în implementarea soluțiilor de securitate informaționala. Confirmarea se va realiza prin prezentarea CV-ului si a studiilor in domeniul securității informaționale.
b. Experiență în cel puțin 3 proiecte similare.
c. Certificat cu Lead Auditor Securitate informaționala conform ISO/IEC 27001:2022 sau echivalent

3.1.2. Expert-cheie nr. 2 - Expert securitate infrastructuri informatice și cloud-uri (LAN, WAN, cloud - Saas, PaaS, IaaS), responsabil de testarea

	infrastructurilor IT, infrastructurilor WAN, LAN., a cloud-urilor (public, private, hybride) și asigurarea consultanței continuă de securizare a acestora. Evaluarea și examinarea vulnerabilităților depistate la nivel de infrastructuri IT și cloud. Raportarea și instruirea echipei de administratori IT ai Beneficiarului. Expertiza se va realiza prin prezentarea CV-ului expertului. Deținător al cetățeniei Republicii Moldova. a. Experiență de cel puțin 10 ani în domeniul securității infrastructurilor informatice. b. Participarea în ultimii 3 ani ca pen-tester la cel puțin 3 contracte similare în domeniul securității infrastructurilor IT complexe, din care cel puțin doua sa fie pe infrastructuri de tip cloud. c.Cunoștințe privind testarea de securitate a cloud-urilor de tip SaaS, PaaS, IaaS din punct de vedere al securității informației, dovedite prin diplome/certificate obținute. (GCPN sau echivalent). d. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite prin diplome/certificate obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent) e. Cunoștințe privind procesul de analiză a vulnerabilităților și interpretarea rezultatelor obținute in urma procesului de scanare și testare efectuat conform unei metodologii recunoscute in domeniu, dovedite prin diploma/certificare eliberata de o instituție cu recunoaștere la nivel național/internațional (ECSA sau echivalent). f. Cunoștințe avansate privind auditul de securitate a sistemelor informatice si evaluarea riscurilor, dovedite prin diplome/certificate obținute (CISA sau echivalent) **3.1.3. Expert-cheie nr. 3 - Expert testare securitate sisteme informatice și aplicații** - este responsabil de testarea de penetrare a sistemelor informatice și a aplicațiilor. Expertiza se va realiza prin prezentarea CV-ului expertului. Deținător al cetățeniei Republicii Moldova. a. Experiența de cel puțin 10 ani în calitate de expert testare securitate sisteme informatice, b. Participarea în ultimii 3 ani la cel puțin 3 contracte similare ca expert în testarea securității sistemelor informatice, c. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere al securității informației, dovedite prin diplome/certificate obținute (CEH sau echivalent), d. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite prin diplome/certificate obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent). e. Cunoștințe privind testarea de securitate a rețelelor de tip Wi-Fi, dovedite prin diplome/certificate obținute (OSWP sau echivalent) **3. Alte cerințe minim obligatorii față de ofertant:** 3.1. Compania ce va presta serviciile de penetrare trebuie să posede o experiență specifică în prestarea serviciilor similar de cel puțin 3 ani în domeniu și minim 3 recomandări , 3 contractare similare pe piața locala din Republica Moldova în ultimii 3 ani. 3.2. Semnarea acordului de confidențialitate ((NDA) Non-Disclosure Agreement) cu compania și echipa de implementarea serviciilor. 3.3.Semnarea declarațiilor de confidențialitate, de fiecare expert nominalizat în echipă. 3.4. Compania ce va presta serviciile de penetrare trebuie să dețină certificările ISO/IEC 27001:2022 cu domeniul de activitate - servicii privind asigurarea securității informației, teste de penetrare si auditarea sistemelor informatice.		

9. În cazul procedurilor de preselecţie se indică numărul minim al candidaţilor şi, dacă este cazul, numărul maxim al acestora. *Nu se aplică*

10. În cazul în care contractul este împărţit pe loturi un operator economic poate depune oferta :

1) Pentru un singur lot.

11. Admiterea sau interzicerea ofertelor alternative: *Nu se admite*
(indicați se admite sau nu se admite)

12. Termenii și condițiile de livrare/prestare/executare solicitați: *Pe parcursul anului 2026.*

13. Termenul de valabilitate a contractului: *31.12.2026*

14. Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): Nu se aplică.

15. Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): Nu se aplică.

16. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse:

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Prezentarea Cererii de participare conform ***Anexei nr.7*** din Ordinul MF 115/2021**.**	Cerere de participare confirmată prin semnătura electronică**.**	***Obligatoriu***
2	Prezentarea Declarației privind valabilitatea ofertei conform ***Anexei nr.8*** din Ordinul MF 115/2021	Declarației privind valabilitatea ofertei confirmată prin semnătura electronică	***Obligatoriu***
3	Prezentarea Specificației de preț conform ***Anexei nr.23*** din Ordinul MF 115/2021	Specificații de preț, confirmat prin semnătura electronică.	***Obligatoriu***
4	Prezentarea Specificații tehnice conform ***Anexei nr.22*** din Ordinul MF 115/2021	Specificații tehnice, confirmată prin semnătura electronică .	***Obligatoriu***
5	Prezentarea Formularul standard al Documentului Unic de Achiziții European completat	Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică	***Obligatoriu***
6	Vor fi excluși operatorii economici care nu și-au îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care este stabilit.	- Accesarea informației privind îndeplinirea obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale de către candidatul sau ofertantul la procedura de atribuire a contractului de achiziții publice se va efectua nemijlocit de către autoritatea contractantă prin accesarea de către autoritățile contractante de pe platforma de interoperabilitate (MConnect), precum și de pe Portalul guvernamental de date, accesând următorul link: https://date.gov.md/open/company-details .	***Obligatoriu lipsa datoriilor - se verifică de CNAS la data deschiderii ofertelor***
7	Vor fi excluși operatorii economici care nu dispun de capacitatea de exercitare a activității profesionale **- existența grupului de proiect calificat asigurat** pentru îndeplinirea serviciilor **- Experiența similară 3 ani**	Prezentarea Declarației de proprie răspundere conform ***Anexei nr.14*** din Ordinul MF 115/2021 privind: - dispunerea grupului de proiect calificat asigurat pentru îndeplinirea serviciilor **1. Cerințe față de membrii echipei de proiect ofertată:** Ofertantul (Prestatorul) trebuie să prezinte dovezi că poate pune la dispoziția Beneficiarului pentru executarea contractului de achiziție publică ce face obiectul prezentei achiziții, un număr minim de experți-cheie, după cum urmează: a. Expert-cheie - Manager de proiect. b. Expert-cheie – Expert 1 - Expert testare securitate infrastructură rețea de diferit tip - Expert testare securitate cloud (public, privat,	***Obligatoriu***

		hybrid) c. Expert-cheie – Expert 2 - Expert testare securitate sisteme informatice - Expert testare securitate aplicații Ofertantul trebuie sa facă dovada îndeplinirii de către experții cheie a următoarelor criterii: **1.1. Expert-cheie nr. 1 - Manager de proiect** este responsabil de gestiunea eficientă a proiectului. Experiența în domeniul protecției datelor cu caracter personal constituie un avantaj. Deținător al cetățeniei Republicii Moldova. a. Experiență de cel puțin 5 ani în implementarea soluțiilor de securitate informațională. Confirmarea se va realiza prin prezentarea CV-ului si a studiilor in domeniul securității informaționale. b. Experiență în cel puțin 3 proiecte similare. c. Certificat cu Lead Auditor Securitate informațională conform ISO/IEC 27001:2022 sau echivalent **1.2. Expert-cheie nr. 2 - Expert securitate infrastructuri informatice și cloud-uri (LAN, WAN, cloud - Saas, PaaS, IaaS)**, responsabil de testarea infrastructurilor IT, infrastructurilor WAN, LAN., a cloud-urilor (public, private, hybride) și asigurarea consultanței continuă de securizare a acestora. Evaluarea și examinarea vulnerabilităților depistate la nivel de infrastructuri IT și cloud. Raportarea și instruirea echipei de administratori IT ai Beneficiarului. Expertiza se va realiza prin prezentarea CV-ului expertului. Deținător al cetățeniei Republicii Moldova. a. Experiență de cel puțin 10 ani în domeniul securității infrastructurilor informatice. b. Participarea în ultimii 3 ani ca pen-tester la cel puțin 3 contracte similare în domeniul securității infrastructurilor IT complexe, din care cel puțin doua sa fie pe infrastructuri de tip cloud. c. Cunoștințe privind testarea de securitate a cloud-urilor de tip SaaS, PaaS, IaaS din punct de vedere al securității informației, dovedite prin diplome/certificate obținute. (GCPN sau echivalent). d. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite prin diplome/certificate obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent) e. Cunoștințe privind procesul de analiză a vulnerabilităților și interpretarea rezultatelor obținute in urma procesului de scanare și testare efectuat conform unei metodologii recunoscute in domeniu, dovedite prin diploma/certificare eliberata de o instituție cu recunoaștere la nivel național/internațional (ECSA sau echivalent). f. Cunoștințe avansate privind auditul de securitate a sistemelor informatice si evaluarea riscurilor, dovedite prin diplome/certificate obținute (CISA sau echivalent) **1.3. Expert-cheie nr. 3 - Expert testare securitate sisteme informatice și aplicații** - este responsabil de testarea de penetrare a sistemelor informatice și a aplicațiilor. Expertiza se va realiza prin prezentarea	

		CV-ului expertului. Deținător al cetățeniei Republicii Moldova. a. Experiența de cel puțin 10 ani în calitate de expert testare securitate sisteme informatice, b. Participarea în ultimii 3 ani la cel puțin 3 contracte similare ca expert în testarea securității sistemelor informatice, c. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere al securității informației, dovedite prin diplome/certificate obținute (CEH sau echivalent), d. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite prin diplome/certificate obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent). e. Cunoștințe privind testarea de securitate a rețelelor de tip Wi-Fi, dovedite prin diplome/certificate obținute (OSWP sau echivalent). **2. experiență specifică în prestarea serviciilor similar de cel puțin 3 ani** în domeniu și minim 3 recomandări , 3 contractare similare pe piața locala din Republica Moldova în ultimii 3 ani.	
8	Vor fi excluși operatorii economici care nu dispun de Standarde de asigurare a calităţii	**1**. Deținerea certificărilor ISO/IEC 27001:2022 cu domeniul de activitate - servicii privind asigurarea securității informației, teste de penetrare si auditarea sistemelor informatice. **2.** Declarație de propria răspundere Operatorului economic în caz de desemnare câștigător se obligă : -Semnarea acordului de confidențialitate ((NDA) Non-Disclosure Agreement) cu compania și echipa de implementarea serviciilor. - Semnarea declaraţiilor de confidenţialitate, de fiecare expert nominalizat în echipă.	
	Va fi exclus din procedura de atribuire a contractului de achiziţii publice orice ofertant sau candidat despre care are cunoştinţă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă și/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu*** *Lipsa condamnării pe parcursul a ultimilor 5 ani.*
9	Va fi exclus orice operator economic care se află în proces de insolvabilitate ca urmare a hotărârii judecătoreşti.	La depunerea ofertei prin declararea în DUAE	***Obligatoriu*** *Nu se află în proces de insolvabilitate*
10	DECLARAŢIE privind confirmarea identității beneficiarilor efectivi și	Declaraţie în conformitate cu **Anexa nr. 1** autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de	***Da*** *– depunere obligatorie după*

	neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani	ofertant/ofertant asociat desemnat câștigător;	*desemnare în calitate de câștigător*

Anexa nr. 1
la Caietul de sarcini

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 145 din 24 noiembrie 2020

DECLARAŢIE
privind confirmarea identității beneficiarilor efectivi şi neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Subsemnatul, _____ reprezentant împuternicit al _____ *(denumirea operatorului economic)* în calitate de ofertant/ofertant asociat desemnat câștigător în cadrul procedurii de achiziție publică nr. _____ din data __/__/___, declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că beneficiarul/beneficiarii efectivi ai operatorului economic în ultimii 5 ani nu au fost condamnați prin hotărâre judecătorească definitivă pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Numele și prenumele beneficiarului efectiv	IDNP al beneficiarului efectiv

Data completării: _____
Semnat: _____
Nume/prenume: _____
Funcţia: _____
Denumirea operatorului economic _____
IDNO al operatorului economic _____

17. Garanția pentru ofertă: Nu se aplică.
18. Garanția de bună execuție a contractului: Nu se aplică.
19. Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrânse și al procedurii negociate), după caz . Nu se aplică.
20. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): licitație electronică, 3 runde, *pasul minim 3 500,00 lei.*
21. Condiții speciale de care depinde îndeplinirea contractului (indicați după ca**z): *Existența grupului de proiect calificat asigurat pentru îndeplinirea serviciilor conform cerințelor din specificația tehnică , deținerea certificărilor ISO/IEC 27001:2022 cu domeniul de activitate - servicii privind asigurarea securității informației, teste de penetrare si auditarea sistemelor informatice. Raportul privind testarea de penetrare, care va include constatările,*

vulnerabilitățile identificate, nivelul de risc și recomandările de remediere, va fi prezentat Beneficiarului cel târziu până la data de 15.12.2026.

22. Ofertele se prezintă în valută: - lei moldovenești**.**

23. Criteriul de evaluare aplicat pentru adjudecarea contractului: *Cel mai mic preț pentru oferta întreagă.*

24. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor: *Nu se aplică*

Nr. d/o	Denumirea factorului de evaluare	Ponderea%
	Nu se aplică	

25. Termenul limită de depunere/deschidere a ofertelor:

- *Conform informației în SIA RSAP* **.**

26. Adresa la care trebuie transmise ofertele sau cererile de participare:
Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP.

27. Termenul de valabilitate a ofertelor: *60 zile*

28. Locul deschiderii ofertelor: *SIA RSAP* **,**
Ofertele întârziate vor fi respinse.

29. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului cînd ofertele au fost depuse prin SIA RSAP.

30. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: *Limba Română.*

31. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: *Nu se aplică*

32. Denumirea și adresa organismului competent de soluționare a contestațiilor:
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md

33. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): Nu se aplică.

34. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: Nu se aplică.

35. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: Nu se aplică..

36. Data transmiterii spre publicare a anunțului de participare: Conform informației în SIA RSAP .

37. În cadrul procedurii de achiziție publică se va utiliza/accepta:

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Nu se acceptă
plățile electronice	Se acceptă

38. Alte informații relevante: *Nu se aplică*

Președinta grupului de lucru: Digitally signed by Moraru Maia
Date: 2026.07.01 09:19:32 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Maia Moraru

L.Ș.