ANUNȚ DE PARTICIPARE INCLUSIV PENTRU PROCEDURILE DE PRESELECȚIE/PROCEDURILE NEGOCIATE

privind achiziționarea: ***Serviciilor de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS pentru anul 2022.***

prin procedura de achiziție: ***Cererea Ofertelor de Pret***

1. **Denumirea autorității contractante:** *Casa Națională de Asigurări Sociale*
2. **IDNO:** *1004600030235*
3. **Adresa:** *mun. Chișinău str. Gheorghe Tudor, 3.*
4. **Numărul de telefon/fax:** *022-257-681; 022-257-551; 022-257-752;*
5. **Adresa de e-mail și pagina web oficială ale 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 prestarea următoarelor serviciilor:**

Cod CPV: 79417000-0 (Servicii de consultanță în domeniul securității)

Lotul nr 1	Servicii testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS	Termen de prestare
1	**Cerințe pentru servicii de testare informatica pentru identificarea și evaluarea vulnerabilităților a infrastructurii IT externe al CNAS.** **1. Scopul și aria de acoperire a serviciilor de pentest:** 1.1.Testarea securității a CNAS se va realiza din extern la nivel de site oficial al organizației, sistemele informaționale publice, are ca scop obținerea unei perspective asupra daunelor potențiale și a riscului de bussines-procesele pe care vulnerabilitățile existente le-ar putea provoca. 1.2.Resursele care sunt expuse testelor de penetrare sunt: 1.2.1. 43 IP adrese externe, oficiile teritoriale. 1.2.2. 8 aplicațiilor web. 1.3. Testele de penetrare externe presupun scopul evaluarea securității a perimetrul extern (expus în Internet) al CNAS, în special pentru sistemele critice conectate la Internet sau accesibile din exteriorul infrastructuri a organizației. În cadrul acestor teste vom evalua orice tip de acces unic din exterior la infrastructura privată al CNAS, inclusiv serviciile care au acces limitat la adrese IP externe individuale. 1.4.Testele de penetrare vor include in mod minimal: a. Obținerea informațiilor din domeniul public b. Scanarea sistemelor din scop c. Tehnici de enumerare - Identificarea sistemelor de operare - Identificarea patch-urilor de securitate lipsa pe un anumit sistem de operare.	**la solicitare Autorității contractante valabil până la 31.12.2022**

- 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

1.5.Metodologia de testare elaborata si folosita de către ofertant va fi în conformitate cu bunele practici internaţionale precum: (OWASP, OSSTMM, ISSAF, NIST, ISACA, etc).

1.6.In realizarea testelor de penetrare, ofertantul va realiza următorii pași:

a. Construirea unui model al amenințărilor. Investigarea arhitecturii infrastructurii si 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, atacuri care ar putea fi realizate, precum si 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. Condițiile unui atac, descrise in modelarea amenințărilor, sunt testate.

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

d. Raportarea rezultatelor. Documentarea problemelor identificate și prezentarea unor recomandări pentru remediere.

1.7.Cerințe fața de testele de penetrare pentru aplicațiile web. Testarea de securitate la nivelul aplicațiilor web este realizata în concordanță cu metodologia OWASP, certificata la nivel mondial. Atacurile din planul de testare vizează în principal următoarele aspecte:

a. Testarea mecanismelor de păstrare a confidențialității si integrității datelor
b. Testarea procesului de Management al Identitarii
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
j. Testarea problemelor de Logica de Business.

1.8.Cerințe fata de descrierea vulnerabilităților identificate. Partea executiva va conține descrierea pe scurt a problemelor si vulnerabilităților identificate si va utiliza metode grafice (cel puțin diagrame, grafice sau harți). Partea tehnica 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 succinta a metodologiei utilizate in cadrul testării;
d. Descrierea contextului în care s-a desfășurat testarea;
e. Prezentarea individuala a vulnerabilităților descoperite, după cum urmează:
- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;

- Descrierea tehnica;
- Analiza severității si probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere.

e. Alte detalii si recomandări;

f. Anexa cu lista testelor de securitate efectuate.

1.9.Cerințe fata de analiza de risc. In 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.

1.10. Cerințe fața de raportul de prezentare și follow-up. 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 beneficiarul testării pe principalele domenii funcționale. De asemenea, în cadrul ședinței va fi prezentat, în forma 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 individuala a vulnerabilităților descoperite, după cum urmează:
- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnica;
- Analiza severității si probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere.
- Alte detalii si 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.

f. Anexa cu lista testelor de securitate efectuate.

1.11. După confirmarea remedierii vulnerabilităților identificate de către beneficiar, ofertantul va realiza o retestare pentru a confirma închiderea vulnerabilităților identificate.

2. Cerințe față de membrii echipei de proiect:

2.1. Compania care va presta serviciile de penetrare trebuie să prezinte dovezi că poate pune la dispoziție un număr minim de experți-cheie precum:

a. Manager de proiect – responsabil de coordonarea echipei de experți și managementului proiectului în sine.

1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Se va/vor prezenta CV-ul acestuia.

b. Expert Securitate sisteme informaționale – responsabil de coordonarea

	echipei de experți în realizarea testelor de penetrare: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Experiența va fi dovedită prin certificat internațional acreditat în calitate de auditor intern securitate informațională ISO 27001, (CISA) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **c. Expert testare securitate infrastructură rețea –** responsabil de testarea de penetrare a infrastructurii de rețea: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. 2. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Offensive Security Certified Professional (OSCP) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **d. Expert testare securitate sisteme informatice –** responsabil de testarea de penetrare a aplicațiilor web: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. 2. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Licensed Penetration Tester (LPT) sau echivalentul, GIAC Cloud Penetration Tester (GCPN) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. 3. Cunoștințe avansate privind sisteme de operare, baze de date, sisteme de virtualizare dovedite prin diplome sau experiența – CV. **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 (sau 3 contractare similare) pe piața locala din R. Moldova în ultimii 3 ani. 3.2. Compania ce va presta serviciile de penetrare trebuie să dețină competență în domeniul de activitate în servicii privind asigurarea securității informației, teste de penetrare și auditarea sistemelor informatice. 3.3. Semnarea acordului de confidențialitate ((NDA) Non-Disclosure Agreement) cu compania și echipa de implementarea serviciilor.	
Valoare estimativă a achiziției lei fără TVA		**350000,00**
Pasul minim de licitare (lei)		**3500,00**

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

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

1) Pentru mai multe loturi.

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

12. Termenii şi condițiile de prestare solicitați ***pe parcursul anului 2022 la solicitarea Beneficiarului îndeplinind cerințele din caietul de sarcini.***

13. Termenul de valabilitate a contractului: *31.12.2022*

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*
(indicați da sau nu)

15. Prestarea serviciului este rezervată unei anumite profesii în temeiul unor legi 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; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1.	Vor fi excluși operatorii economici care nu și-au îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit.	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertei) - eliberat de Inspectoratul Fiscal Principal de Stat, confirmat prin semnătura electronică, ori link-ul la accesarea unei baze de date naționale disponibile gratuit pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor.	***Obligatoriu***
2.	Vor fi excluși operatorii economici care nu dispun de capacitatea economică și financiară ofertantului; Cifra de afaceri în activitatea similară în ultimii 3 ani minimum 350 000,00 lei pentru fiecare an.	La depunerea ofertei prin declararea în DUAE/ la evaluare Declaraţii privind cifra de afaceri în domeniul de activitate aferent obiectului contractului (prestarea serviciilor similare) conform ***Anexei nr.12*** din Ordinul MF 115/2021 într-o perioadă anterioară care vizează activitatea pentru ultimii minim 3 ani - *a cîte min 350 000,00 lei pentru fiecare din ultimii 3 ani* original confirmat prin semnătura electronică a participantului. la solicitare se va prezenta documente primare de confirmare a nivelului serviciilor propuse.	***Obligatoriu*** *în cazul existenței datelor cu caracter personal sau informațiilor care prezintă secret comercial informația se remite direct autorității contractante pe poșta electronică achizitiicnas@cnas.gov.md*
3.	Vor fi excluși operatorii economici care nu dispun de capacitatea tehnică și profesională –minimum 3 ani de experiența similară – existența echipei de proiect calificat asigurat pentru îndeplinirea serviciilor relevante.	- Lista principalelor prestări similare efectuate în ultimii minim 3 ani, conținînd valori, perioade de prestare, beneficiari, prezentare minimum 3 recomandări (sau 3 contractare similare) pe piața locala din R. Moldova în ultimii 3 ani - Declarația de proprie răspundere conform ***Anexei nr.14*** din Ordinul MF 115/2021 privind: - dispunerea echipei de proiect calificat asigurat pentru îndeplinirea serviciilor relevante. **Cerințe față de membrii echipei de proiect:** . Compania care va presta serviciile de penetrare trebuie să prezinte dovezi că poate pune la dispoziție un număr minim de experți-cheie precum: **a. Manager de proiect –** responsabil de coordonarea echipei de experți și managementului proiectului în sine. 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Se va/vor prezenta CV-ul acestuia. **b. Expert Securitate sisteme informaționale –** responsabil de coordonarea echipei de experți în realizarea testelor de penetrare: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. Experiența va fi dovedită prin certificat internațional acreditat în calitate de auditor intern securitate informațională ISO 27001, (CISA) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **c. Expert testare securitate infrastructură rețea –** responsabil de testarea de penetrare a infrastructurii de rețea: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie.	***Obligatoriu*** *în cazul existenței datelor cu caracter personal sau informațiilor care prezintă secret comercial informația se remite direct autorității contractante pe poșta electronică achizitiicnas@cnas.gov.md*

		2. Cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Offensive Security Certified Professional (OSCP) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. **d. Expert testare securitate sisteme informatice –** responsabil de testarea de penetrare a aplicațiilor web: 1. Experiență de cel puțin 3 ani în proiecte similare ca și complexitate și arie. 2. Cunoștințe privind testarea de securitate a sistemelor informatice din punct de vedere a securității informaționale dovedite prin diplome sau certificate precum: Licensed Penetration Tester (LPT) sau echivalentul, GIAC Cloud Penetration Tester (GCPN) sau echivalentul. Se va/vor prezenta CV-ul acestuia/ora. 3. Cunoștințe avansate privind sisteme de operare, baze de date, sisteme de virtualizare dovedite prin diplome sau experiența – CV.	
4.	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 hotărîrea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă şi/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor şi alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu***
5.	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***

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): licitația electronică, 3 runde , pasul minim pentru întreaga ofertă 3500.00 lei.

21. Condiții speciale de care depinde îndeplinirea contractului (indicați după caz**): nu sunt**

22. Ofertele se prezintă în valuta: - lei moldovenești.

23. Criteriul de evaluare aplicat pentru adjudecarea contractului: ***Cel mai mic preț fără TVA pentru întreaga ofertă.***

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 când ofertele au fost depuse prin SIA RSAP.

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

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: BAP, nr.82 din data 22.10.2021**.**

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. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): *Nu se aplică*

39. Alte informații relevante:

Digitally signed by Moraru Maia
Date: 2022.11.03 11:00:44 EET
Reason: MoldSign Signature
Location: Moldova

Președintele grupului de lucru: _____ Maia Moraru

L.Ș.