ANUNȚ DE PARTICIPARE

Privind achiziționarea *Resurselor informaționale pentru politica de securitate informațională a CNAS (servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT) și instruirea profesională a personalului CNAS în domeniul securității cibernetice pe parcursul anului 2021.*

prin procedura de achiziție: *Licitația Publică*

Denumirea autorității contractante: *Casa Națională de Asigurări Sociale*

1. **IDNO:** *1004600030235*
2. **Adresa:** *mun. Chişinău, str. Gh. Tudor,3, bir. № 515*
3. **Numărul de telefon/fax: (***022)257-681; 257-551*
4. **Adresa de e-mail și de internet a autorității contractante:** *achizitiicnas@cnas.gov.md*
5. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire: *documentația de atribuire este anexată în cadrul procedurii în M-Tender SIA RSAP2***
6. **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): Autoritatea publică centrală**
7. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind prestarea următoarelor servicii:**
   Cod CPV: (79417000-0) Servicii de consultanţă în domeniul securităţii

Nr.	Denumirea obiectului achiziției	Specificațiile tehnice
1	2	3
1.1.	Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități lunare, consultanță, testare a securității cibernetice din cadrul CNAS)	**Specificațiile tehnice obiectului achiziției.** • Scanări de vulnerabilități lunare conform standardelor internaționale cu instrumente speciale. Analiza vulnerabilităților sistemelor informaționale CNAS (inclusiv din Cloud) și identificarea celor adevărate din cele false. Raportarea lunară 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. • 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. • 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. Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea

		vulnerabilităților existente și cunoscute intr-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferența ca acestea vor fi efectuate intr-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. **Scopul serviciilor prestate:** • asigurarea unui climat funcțional și protejat al sistemului informațional, precum și asigurarea cerințelor minime obligatorii de securitate cibernetică pentru instituțiile de stat. • monitorizarea procesul de securizare continuu a sistemelor informatice de către experți ai Prestatorului și raportarea lunară existența/apariția vulnerabilităților în contextul sistemului informațional cu o dinamică avansată și complexă. • creșterea vigilenței la incidente de securitate cibernetică prin pregătire,. Îndeplinirea cerințelor față de servicii din ***Anexa nr. 1*** Ca urmare a serviciilor prestate, Prestatorul va oferi livrabilele conform ***Anexei nr.2***
	Valoare estimativă Poziția 1.1.	**700 000,00**
1.2.	Instruirea profesională a personalului CNAS în domeniul securitatății cibernetice pe parcursul anului 2021	**1. Domeniul instruirii de dezvoltare profesională** **-"Securitate cibernetică"** **2.Tipul de instruire** Internă **3. Obiectivele generale de dezvoltare profesională referitoare la cunoştinţele care trebuie să fie acumulate şi abilităţile care trebuie să fie dezvoltate de către funcţionarii publici în urma participării acestora la activităţile de instruire** Îmbunătăţirea cunoştinţelor participanţilor la activitatea de instruire privind securitatatea cibernetică, riscurilor actuale de compromitere a informaţiilor din interior. Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică, etc. 4. **Subiectele/tematicile de instruire obligatorii de a fi examinate** - Formarea culturii securităţii cibernetice; - Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică; - Conştientizarea riscurilor actuale de compromitere a informaţiilor din interior (sustragere, copiere, distrugere, divulgare, scurgere) şi impactul acestora; - Modalităţi şi reguli de setare a parolelor, precum şi asimilarea tehnicilor de igienă cibernetică în procesul de activitate. 5. **Durata acceptată pentru activităţile de instruire** Minim 2 ore academice de instruire per grup pentru specialiştii CNAS (utilizatori de sisteme informaţionale); Minim 2 ore academice de instruire pentru conducerea CNAS; Minim 8 ore academice de instruire per grup pentru specialiştii din domeniul tehnologii informaţionale. 6. **Informaţia succintă privind grupul-ţintă pentru care se organizează instruirea** a) **Categoria de participanţi** - Specialiştii CNAS (utilizatori de sisteme informaţionale). - Conducerea CNAS. - Specialişti din domeniul tehnologii informaţionale. b) **Domeniul de competenţă al participanţilor** Administrarea şi gestionarea eficientă a sistemului public de asigurări sociale. c) **Numărul de participanţi** 1. **1235** participanţi - utilizatori de sisteme informaţionale (62 grupe).

		2. **4** participanţi – conducerea CNAS (1 grup). 3. **57** participanţi – specialişti din domeniul tehnologii informaţionale (3 grupe). d) **Informaţia privind preferinţele din punctul de vedere al realizării programelor de instruire** - Realizarea activităţilor de instruire online, după caz, în contextul situaţiei epidemiologice din Republica Moldova; - Testarea practică a angajaţilor prin diverse tehnici de manipulare la disponibilitatea de a oferi date tehnice interne persoanelor terţe – inginerie socială, cu întocmirea unui Raport a testării angajaţilor. - Elaborarea și furnizarea materialelor de suport participanților la curs; - Adaptarea programului de instruire elaborat iniţial la necesităţile specifice ale angajaţilor/CNAS, îl prezintă conducerii CNAS spre aprobare şi îl realizează în strictă conformitate cu contractul încheiat; - Evaluarea cursului de instruire și întocmirea Raportului privind activitatea de instruire. - Folosirea stilului interactiv de instruire, evitând sesiunile teoretice de lungă durată. Cursul de instruire se va desfășura în limba română. **Profilul prestatorului de servicii** Serviciile de instruire urmează a fi oferite de către specialişti în domeniul protecţiei datelor cu caracter personal, experţi în securitatea cibernetică. **Criterii minime de calificare:** •Diplomă/certificate de studii a formatorului/formatorilor în domenii relevante serviciilor prestate; •Experiență în prestarea serviciilor de dezvoltare profesională în domeniul în care se organizează activitatea de dezvoltare profesională menționată. **Procedura de aplicare:** În vederea demonstrării conformității cu cerințele solicitate, aplicantul va prezenta: • Programul de instruire în corespundere cu cerinţele expuse de CNAS •Scrisoarea de intenţie a formatorului care să cuprindă informații cu privire la rezultatele activității anterioare în domeniul prestării serviciilor de dezvoltare profesională de domeniu (descrierea succintă a celor mai relevante activități de instruire realizate); •Curriculum vitae a formatorului care va cuprinde informații cu privire la experiența în prestarea serviciilor de dezvoltare profesională în domeniul în care se organizează activitatea de dezvoltare profesională menționată. •Copie a diplomei/certificatelor de studii a formatorului; •Copie a actelor de identitate ale formatorului; •Oferta financiară (în lei MDL) privind onorariul solicitat pentru îndeplinirea sarcinilor care revin. **Declarație de confidențialitate** Toate datele și informațiile primite de la personalul Casei Naționale de Asigurări Sociale pentru realizarea obiectivului acestei sarcini trebuie tratate confidențial și pot fi utilizate doar în legătură cu executarea activităților descrise în prezentul Caiet de sarcini.
	Valoare estimativă Poziția 1.2.	**300 000.00**
Valoare estimată: lei fără TVA		**1 000 000,00**

Anexa nr.1

Cerințele față de servicii :

1.Serviciile de scanări de vulnerabilități lunare 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 Prestatorului vulnerabilitățile cu pericol sporit de securitate și fiecărei

vulnerabilități îi vor fi atribuite recomandări de fixare. Fiecare scanare lunară de vulnerabilități va genera un Raport lunar de vulnerabilități prezentat și explicat în detalii conducerii Autorității contractante.

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 Prestatorului a implementării corecte și setării suficiente a ecranelor de protecție gen firewall la nivel de stații, servere, echipamente de rețea, etc.

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 - in aceasta situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicațiilor (pagini web, adrese IP). Aceasta metoda va fi utilizata pentru testarea 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 (VPN). Testarea din interior a infrastructurii va include minim vectorii de atac în scop de re-evaluare a testului de penetrare precedent.

4. Prestatorul va utiliza 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).

5. Prestatorul va deține 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.

6. Prestatorul va deține proceduri de lucru conforme standardelor in domeniu, prin care este redus riscul de a afecta sistemele informatice aflate in scopul testării.

Anexa nr. 2

Cerințe față de livrabilele proiectului:

Ca urmare a serviciilor prestate, Prestatorul va oferi:

- Plan de proiect;
- Plan de scanări și testare;
- Planul de acțiuni (SOW - Scope of Work);
- Rapoartele de scanări de vulnerabilități care vor include vulnerabilitățile detectate, catalogate in 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, va 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.

Rapoartele furnizate de Prestator vor fi structurate în două părți distincte:

a) Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice.

b) Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate. Partea tehnica va conține cel puțin următoarele capitole:

- Sumar executiv;
- Obiectivele și scopul evaluării;
- Prezentarea metodologiei utilizate in cadrul testării;

- Descrierea contextului in care s-a desfășurat testarea;
- Detalii despre rețeaua și sistemele evaluate:
  - echipamentele și serviciile active (adrese IP, porturi deschise,)
  - tipul , versiunea, statutul actualizărilor aplicațiilor
  - sistemul de operare
- Prezentarea individuala 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;
- Anexa cu lista testelor de securitate efectuate.

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

8. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):**

1) Pentru întreaga ofertă;

9. **Admiterea sau interzicerea ofertelor alternative:** Nu se admite

10. **Termenii și condițiile de prestare serviciilor:** ***serviciile se prestează timp de 8(opt) luni începînd cu 01.05.2021 pînă la 31.12.2021, acte de îndeplinire a serviciilor se prezintă dupa prestarea lor pentru acceptarea de către Beneficiar.***

11. **Termenul de valabilitate a contractului:** *31.12.2021*

12. **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

13. **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

14. **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):**

	Denumirea documentului/cerinţelor	***Mod de demonstrare a îndeplinirii cerinţei:***	***Obl. Da /Nu***
1	oferta	Document scanat - confirmat prin semnătura electronică a participantului conform Formularului (F 3.1)	***Da***
2	Specificații de preț	Document scanat - conform F4.2 din Documentația Standard, confirmat prin semnătura electronică a participantului.	***Da***
3	Specificații tehnice	Document scanat - conform F4.1 din Documentația Standard, - confirmat prin semnătura electronică a participantului.	***Da***
4	Garanţia pentru oferta 1%	1.00% din valoarea ofertei fără TVA Document scanat - confirmat prin semnătura electronică a participantului.	***Da***

5	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertelor)	Document scanat eliberat de Inspectoratul Fiscal - confirmat prin semnătura electronică a participantului	***Da***
6	Formularul standard al Documentului Unic de Achiziții European	Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică a Participantului	***Da***
7	Demonstrarea capacităţii economice şi financiare a operatorului economic	- Declaraţia de proprie răspundere privind cifra de afaceri în domeniul de activitate aferent obiectului contractului într-o perioadă anterioară care vizează activitatea din ultimii 3 ani, cifra de afaceri anuală pentru ultimii 3 trei ani minimum 500 000.00 - confirmat prin semnătura electronică a participantului. - Minimum ani de experienţă specifică în prestarea serviciilor similare - 3 ani. Experiența minimă în domeniul confirmată prin lista principalelor servicii similare prestate în ultimii 3 ani, conținând valori, perioade de prestare, beneficiari. Prestările de servicii se confirmă prin prezentarea unor contracte de prestarea serviciilor similare - confirmat prin semnătura electronică a participantului.	***Da***
8	Demonstrarea capacitatea profesională a operatorului economic	**Pentru poziția 1.1** Confirmată prin existenţa grupului de experți calificați pentru asigurarea îndeplinirii calitative serviciilor solicitate - informaţii referitoare la personalul de specialitate de care dispune sau al cărui angajament de participare a fost obţinut de către ofertant după cum urmează; Cerințe minime pentru echipa de experți: A. Expert cheie nr.1 - Manager de proiect: responsabil de gestiunea eficientă a proiectului. Experiența în domeniul protecției datelor cu caracter personal. Experiență de cel puțin 5 ani în calitate de manager de proiect pe proiecte in securitate cibernetică. Experiență în cel puțin 3 proiecte similare cu proiectul CNAS ca complexitate și arie. B. Expert cheie nr.2 de testare securității infrastructurii rețelelor de diferit tip, cloud (public, privat, hybrid), cloud-uri (LAN, WAN, cloud - Saas, PaaS, IaaS), sistemelor informatice, testarea infrastructurilor IT, infrastructurilor WAN, LAN, 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. Experiență de cel puțin 5 ani în domeniul securității infrastructurilor informatice. Participarea in ultimii 2 ani ca auditor tehnic sau pen-tester la cel putin 3 contracte similare în domeniul securității infrastructurilor IT și a cloud-urilor Confirmate prin: - diplome/certificate obținute (CCSP sau echivalent); - diplome/certificate obținute în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic (CEH Practic, LPT Practic, OSCP sau echivalent); - diploma/certificare eliberata de o instituție cu recunoaștere la nivel național/internațional	***Da***

		(ECSA sau echivalent). C. Experți cheie nr.3 de testare securitate sisteme informatice și aplicații responsabili de testarea de penetrare a sistemelor informatice și a aplicațiilor. Experiența de cel puțin 5 ani in calitate de expert testare securitate sisteme informatice. Participarea în ultimii 2 ani la cel puțin 3 contracte similare ca expert in testarea securității sistemelor informatice Confirmate prin: - diplome/certificate obținute (CEH sau echivalent); - diplome/certificate obținute (CISSP sau echivalent); - diplome/certificate obținute (CSSLP sau echivalent); - diplome/certificate obținute (precum Microsoft/Linux, Oracle, VMWare sau echivalent) **Pentru poziția 1.2** - Confirmative privind existența experienței în prestarea serviciilor de dezvoltare profesională în domeniul ”Securității cibernetică” ori analogică.	

15. Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrînse și al procedurii negociate), după caz .

16. **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 10 000.00 lei***

17. Condiții speciale de care depinde îndeplinirea contractului : nu se aplică

18. Criteriul de evaluare aplicat pentru adjudecarea contractului: *Cel mai mic preț fără TVA pe oferta întreagă*

19. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor:

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

20. Termenul limită de depunere/deschidere a ofertelor:

- **până la:** *Conform informației în SIA RSAP 2, M-Tender.*

21. Adresa la care trebuie transmise ofertele sau cererile de participare:

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP 2, M-Tender

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

23. Locul deschiderii ofertelor: *SIA RSAP 2, M-Tender*
Ofertele întîrziate vor fi respinse.

24. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții nu participă la deschiderea ofertelor, deoarece ofertele urmează să fie depuse prin SIA RSAP 2, M-Tender

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

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

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

28. **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**

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

30. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:__** sit-ul CNAS www.cnas.md.

31. **Data transmiterii spre publicare a anunțului de participare:** Conform informației în SIA RSAP 2, M-Tender.

32. **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

33. **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**

34. **Alte informații relevante:**

Președinte grupului de lucru: _____ **Maia MORARU**

Digitally signed by Moraru Maia
Date: 2021.03.23 13:12:54 EET
Reason: MoldSign Signature
Location: Moldova

L.Ș.