ANUNȚ DE PARTICIPARE

privind achiziționare a ***serviciilor cu privire la realizarea în cadrul sistemului informațional CNAS a testului de vulnerabilitate (penetration test)***

prin procedura de achiziție *Cererea ofertelor de preț*

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; -257-551*
5. **Adresa de e-mail și de internet a autorității contractante:** *achizitiicnas@cnas.gov.md*
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire:** ***documentația de atribuire sunt anexate în cadrul procedurii în M-Tender SIA RSAP 2***
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):** *Autoritate publică centrală*
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea următoarelor bunuri:**

Codul CPV: **72254000-0 (Testare de software)**

Nr. d/o	Cod CPV	Denumirea serviciilor solicitate	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată, lei fără TVA	Pasul minim
Lotul I						
1	**48000000-8**	Servicii de realizare în cadrul sistemului informațional CNAS a testului de vulnerabilitate (penetration test)	1 serviciul	***Conform cerințelor din Anexa nr. 1***	290 000,00	2 900,00

Anexa nr. 1

Cerințe către servicii a testului de vulnerabilitate (penetration test)

1.1. Cerințele față de serviciile de penetrare

1.1.1. Serviciile de penetrare vor avea ca rezultat o analiză complexă a securității infrastructurii informatice ale Beneficiarului, testînd eficacitatea măsurilor 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 vor fi următoarele:

a.***Black box*** – în această situație echipa de testare nu va cunoaște nici o informație despre sistemele auditate, cu excepția informației de accesare a aplicațiilor (pagini web, adrese IP). Această metodă va fi utilizată pentru testarea infrastructurii externe a Beneficiarului.

1.1.2. Ofertantul va trebui să utilizeze echipamente și aplicații, și să dețină experiență pentru realizarea de teste de penetrare la nivel de rețea, inclusiv wireless, sistem de operare, baze de date și aplicații, inclusiv cele web, atacuri informatice simulînd aplicații malițioase, cît și de negare a serviciului (DoS).

1.1.3. Ofertantul va trebui să dețină și să utilizeze echipamente și aplicații dedicate pentru identificarea și obținerea informațiilor despre sistemele informatice țintă, identificarea de vulnerabilități, și formularea unor recomandări de remediere.

1.1.4. Ofertantul va trebui să dețină proceduri de lucru conforme standardelor în domeniu, prin care este redus riscul de a afecta sistemele informatice aflate în scopul testării.

1.2. Cerințe față de etapele procedurii de evaluare și testare.

Serviciile de penetrare și evaluare a vulnerabilităților tehnice în cadrul infrastructuii informatice ale Beneficiarului prin teste specifice de penetrare din exteriorul infrastructurii de rețea se vor derula în trei etape distincte, și anume:

1. Pre-evaluare (Pre-assesment)

2. Evaluare (Assesment)

3. Post-evaluare (Post-assesment)

1.2.1. ***Etapa de Pre-evaluare(Pre-assesment)*** - reprezintă faza premergătoare evaluării vulnerabilităților și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării.

În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni(Scope of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor de penetrare.

Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni în care se vor înscrie cel puțin:

- activitățile întreprinse,
- sistemele incluse în activitatea de testare,
- termenul propus de realizare,
- persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului.

1.2.2. ***Etapa de Evaluare (Assesment)*** - reprezintă etapa de identificare și evaluare a vulnerabilităților de securitate a infrastructurii informatice.

Această etapă a testării include evaluarea conectivității între sistemele utilizate pentru test și sistemele testate, culegerea informațiilor despre sistemele testate din domeniul public și privat, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților.

Utilizînd informațiile descoperite în evaluarea vulnerabilităților, se vor construi arbori de atac și se vor implementa acțiunile definite în aceste structuri.

Scanarea vulnerabilităților și implementarea testului de penetrare va include, dar nu se va limita la analiza următoarelor vulnerabilități ale aplicațiilor:

- Injectarea de cod malițios;
- Managementul defectuos al procesului de autentificare și al sesiunii de lucru
- Cross-Site Scripting (XSS);
- Referențierea directă a obiectelor în mod nesecurizat;
- Erori privind configurația de securitate;
- Tratarea erorilor în mod nesecurizat și lipsa de măsuri de protecție a informațiilor sensibile;
- Controale ineficiente privind managementul accesului;
- Cross-Site Request Forgery (CSRF);
- Utilizarea de componente de sistem cu vulnerabilități cunoscute;
- Validarea parametrilor de intrare ai aplicațiilor;
- Comportamentul aplicațiilor/sistemelor aflate în scop la un atac de tip Denial of Service (DoS);

În privința managementului sesiunii de lucru se vor identifica cel puțin următoarele aspecte:

- Implementarea managementului sesiunii printr-un Framework cunoscut și de încredere, care a fost testat în practică din punct de vedere al securității;
- Procesul de generare a identificatorilor de sesiune și protecția acestora împotriva abuzurilor;
- Procesul de generare a cookie-urilor ce conțin generatori de sesiune și stabilire a atributelor acestora;
- Procesul de creare și terminare a sesiunii și identificatorilor din perspectiva server și client;
- Intervaluri de inactivitate și posibilitatea de inițializare de multiple sesiuni active;
- Măsurile implementate pentru păstrarea confidențialității informațiilor privind autentificarea și sesiunea de lucru;
- Implementarea de măsuri adiționale de securitate pentru operațiile sensibile, precum cele administrative;

În privința configurației de securitate se vor identifica cel puțin următoarele aspecte:

- Versiunile de Software ale serverelor, platformelor de dezvoltare a aplicației și componentelor sistemului;
- Existența actualizărilor de securitate aflate pe serverele, platformele de dezvoltare a aplicației și componentele sistemului;
- Existența configurațiilor prestabilite de la producătorul sistemului, cum ar fi utilizatori și parole implicite;
- Utilizatorii de aplicații și configurația acestora;
- Metodele și extensiile protocolului HTTP folosite în cadrul sistemului;

- Informații relevante ce se afla în header-ul HTTP;
- Existența mecanismelor de criptare pentru autentificarea în cadrul sistemelor și transmisia de informații;

În privința tratării erorilor de sistem și protejării informațiilor sensibile se vor identifica cel puțin următoarele aspecte:

- Identificarea posibilității ca aplicațiile să divulge informații sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informații despre cont, în mesaje de erori;
- Conținutul mesajelor de eroare din punct de vedere tehnic.

În privința managementului accesului se vor identifica cel puțin următoarele aspecte:

- Procesul de identificare, autentificare si autorizare a accesului la informații;
- Identificarea credențialelor hard-codate în sisteme, dacă acestea există;
- Identificarea utilizatorilor și credențialelor de acces stocate în fișiere de configurație în clar;
- Identificarea credențialelor transmise in clar, daca este cazul;
- Identificarea rolurilor de acces și maparea acestora pe drepturi și posibilitatea de ocolire a acestora pentru a obține acces neautorizat la informații;
- Identificarea metodelor HTTP folosite în procesul de autentificare.

În privința validării parametrilor de intrare se vor identifica cel puțin următoarele aspecte:

- Filtrarea și validarea datelor provenite din afara sistemelor;
- Existența unei metode centralizate de validare a datelor în sistem;
- Existența unor seturi de caractere corespunzătoare pentru datele de intrare;
- Codificarea datelor într-un set comun de caractere înainte de validare;
- Validarea datelor provenite de la utilizatori, înainte de procesarea acestora, inclusiv toți parametrii, conținutul URL si HTTP.

Pentru validarea datelor de intrare se vor verifica:

- tipurile de date așteptate (integer, string etc.);
- setul de date;
- lungimea datelor;
- Implementarea de măsuri suplimentare de control pentru caractere cu potențial riscant (<> " ' % ( ) & + \ \' \");

Testarea securității la nivelul infrastructurii Wireless (WiFi) va include, dar nu se va limita la:

- Descoperirea rețelelor WiFi și punctelor de acces atît cunoscute cît și neautorizate;
- Identificarea dispozitivelor care interacționează cu rețeaua;
- Colectarea de informații despre puterea de rețea, protocoale de securitate și a dispozitivelor conectate;
- Atacul și penetrarea rețelelor criptate cu WEP, WPA-PSK si WPA2-PSK;
- Impersonare SSID;
- Atacuri de tip Man-in-the-middle;
- Monitorizare automată trafic pentru a găsi fluxuri de date sensibile;
- Aderarea la rețelele compromise și testarea sistemelor de Backend;
- Raportare cuprinzătoare a activităților de testare a rețelelor de tip WiFi.

Scanarea vulnerabilităților și implementarea testului de penetrare la nivelul rețelei va include, dar nu se va limita la :

- Obținerea informațiilor din domeniul public;
- Scanarea sistemelor din Planul de acțiuni;
- Tehnici de enumerare;
- Obținerea accesului neautorizat prin exploatarea vulnerabilităților;
- Consolidarea accesului;
- Ștergerea tuturor fișierelor utilizate în cadrul atacului și a altor dovezi ale accesului;
- Aplicații software utilizate în cursul testării;
- Aplicații pentru culegerea de informații din domeniul public;
- Aplicații necesare identificării sistemelor și serviciilor active;
- Scannere de vulnerabilități specifice sistemelor și rețelelor incluse în Planul de acțiuni;
- Aplicații necesare exploatării vulnerabilităților descoperite.

Prin testarea automată va trebui să se detecteze cel puțin următoarele tipuri de vulnerabilități:

- Parole inițiale neschimbate pe echipamente;
- Posibilitatea de acces în sistem fără autentificare, cu autentificare cu credențiale inițiale sau credențiale ușor de ghicit;
- Configurații inițiale neschimbate pe echipamente;
- Corecții și actualizări de securitate neimplementate;
- Escaladarea privilegiilor;
- Software cu versiuni vechi și foarte vechi ce prezintă vulnerabilități;
- Buffer Overflow;
- Negarea accesului la serviciu (DoS Denial of Service);
- Remote Code Execution;
- Posibilitatea injectării de comenzi sau scripturi în servere web, servere de aplicații și baze de date;
- Directory Traversal;
- File and Path Disclosure;
- Cross Site Scripting;

- Cross Site Request Forgery;
- Configurarea defectuoasă a serverelor;
- Managementul defectuos al sesiunilor și autentificării;
- Parametri de intrare nevalidați;
- Control al accesului defectuos;
- Tratarea defectuoasă a erorilor.

Soluția de testare automată utilizată trebuie să fie capabilă să integreze capabilitățile de descoperire și remediere a vulnerabilităților cu informații despre *aplicațiile Malware*prezente în infrastructură, cît și toate aplicațiile Malware cunoscute cu ajutorul cărora se pot exploata vulnerabilitățile prezente și ușurința cu care aceste vulnerabilități se pot exploata.

Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de test care vor include toate problemele și vulnerabilitățile descoperite pe parcursul testării.

1.2.3***Etapa de Post-evaluare (Post-assesment)***- această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea de către Prestator a rapoartelor de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact.

În această etapă Prestatorul va acorda suport Beneficiarului pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora (din cadrul celor propuse), în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite. Totodată Prestatorul va efectua test de penetrare repetat la resursele cu probleme identificate pentru a verifica daca au fost aplicate corect măsurile/metodele de remediere.

1.3. Cerințe față de livrabilele proiectului

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

- Plan de proiect;
- Plan de testare;
- Planul de acțiuni (Scope of Work);
- Rapoarte de test care vor include toate problemele și vulnerabilitățile detectate pe parcursul testării, catalogate în funcție de gravitatea lor;
- 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.

Rapoartele furnizate de Prestator vor fi structurate în două părți distincte:
- partea executivă,
- partea tehnică.

Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice.
Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate.
Partea tehnică va conține cel puțin următoarele capitole:

- Sumar executiv;
- Obiectivele și scopul evaluării;
- Prezentarea metodologiei utilizate în cadrul testării;
- Descrierea contextului în care s-a desfășurat testarea;
- Detalii despre rețeaua și sistemele evaluate:
  - echipamentele și serviciile active (adrese IP, porturi deschise);
  - Tipul, versiunea, statusul actualizărilor aplicațiilor
  - Sistemul de operare;
- 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;
- 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.

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

Pentru întreaga ofertă

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

11. **Termenii și condițiile de prestare a serviciilor solicitate:** *începerea prestării serviciului în termen de pînă la 15 zile din data înaintării comunicării către operatorul economic privind transmiterii dării de seama la Agenţia Achiziţii Publice, durata de executarea a testărilor max. 60 zile.*

12. **Termenul de valabilitate a contractului :** *31.12.2020*

13. **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

14. **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

15. **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 participantului.	*Da*
3	Specificații tehnice	Document scanat - conform F4.1 din Documentația Standard, - confirmat prin semnătura electronică participantului.	*Da*
4	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertelor)	copie – eliberat de Inspectoratul Fiscal - document scanat - confirmat prin semnătura electronică a participantului	*Da*
5	Formularul standard al Documentului Unic de Achiziții European	Formularul standard al Documentului Unic de Achiziții European (DUAE) - document scanat - confirmat prin semnătura electronică a participantului	*Da*

16. **Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrînse și al procedurii negociate), după caz .** Nu se aplică

17. **Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică):** *licitația electronic. Numărul de runde – 3.. Pas minim – 2900.00 lei.*

18. **Condiții speciale de care depinde îndeplinirea contractului (**indicați după caz**):** *nu se aplică*

19. **Criteriul de evaluare aplicat pentru adjudecarea contractului:** *cel mai mic preț fără TVA.*

20. **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	

21. **Termenul limită de depunere/deschidere a ofertelor:**
    - Conform informației în SIA RSAP 2, M-Tender
22. **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
23. **Termenul de valabilitate a ofertelor:** *30 zile*
24. **Locul deschiderii ofertelor:** *SIA RSAP 2, M-Tender.*
    Ofertele întîrziate vor fi respinse.
25. **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".
26. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:**
    Limba de stat
27. **Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene:** Nu se aplică
28. **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
29. **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
30. **În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare:** Nu se aplică
31. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:** Nu se aplică
32. **Data transmiterii spre publicare a anunțului de participare:** Conform informației în SIA RSAP 2, M-Tender.
33. **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

34. **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
35. **Alte informații relevante:** _____

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

L.Ș.