Anexa nr.1
la Ordinul ministrului finanţelor

nr. 115 din 15.09.2021

DOCUMENTAŢIA STANDARD
pentru realizarea achizițiilor publice de bunuri și servicii

INSTRUCŢIUNI PENTRU AUTORITĂȚI CONTRACTANTE ȘI OFERTANŢI

Secţiunea 1

Dispoziții generale

1. Prezenta Documentaţie reprezintă o instrucțiune pentru autoritățile contractante și ofertanți, utilizată la inițierea și desfășurarea procedurilor de achiziţii publice de bunuri și servicii. La procedurile de achiziţii de bunuri și servicii iniţiate şi desfăşurate prin cererea ofertelor de preţuri şi achiziţiile de valoare mică, autorităţile contractante pot simplifica formularele în dependenţă de complexitatea achiziţiei.

2. Prezenta Documentație conține anexe destinate inițierii, publicării, atribuirii și modificării procedurilor de achiziții publice, precum și destinate să faciliteze elaborarea și prezentarea ofertei, și a documentelor care să permită grupului de lucru examinarea şi evaluarea tuturor ofertelor depuse, după cum urmează:

1) Anunț de intenție (anexa nr.1);
2) Anunț de participare, inclusiv pentru procedurile de preselecție/procedurile negociate (anexa nr. 2);
3) Invitație de participare la etapele de preselecție/la procedurile negociate (anexa nr. 3);
4) Proces-verbal cu privire la rezultatele preselecției candidaților (anexa nr. 4);
5) Anunț de atribuire (anexa nr. 5);
6) Anunț privind modificarea contractului de achiziții publice/acordului-cadru (anexa nr. 6);
7) Cerere de participare (anexa nr. 7);
8) Declaraţie privind valabilitatea ofertei (anexa nr. 8);
9) Scrisoare de garanţie bancară (anexa nr. 9);
10) Garanţia de bună execuţie (anexa nr. 10.);
11) Informaţii privind asocierea (anexa nr. 11);
12) Declarație privind lista principalelor livrări/prestări efectuate în ultimii 3 ani de activitate (anexa nr. 12);
13) Declaraţie privind dotările specifice, utilajul şi echipamentul necesar pentru îndeplinirea corespunzătoare a contractului (anexa nr. 13);
14) Declaraţie privind personalul de specialitate propus pentru implementarea contractului (anexa nr. 14);
15) Lista subcontractanților şi partea/părţile din contract care sunt îndeplinite de aceştia (anexa nr. 15);
16) Angajament terţ susţinător financiar (anexa nr. 16);
17) Declaraţie terţ susţinător financiar (anexa nr. 17);
18) Angajament privind susținerea tehnică și profesională a ofertantului/grupului de operatori economici (anexa nr. 18);
19) Declaraţie terţ susţinător tehnic (anexa nr. 19);
20) Declaraţie terţ susţinător profesional (anexa nr. 20);

21) Caiet de sarcini (anexa nr. 21);
22) Specificaţii tehnice (anexa nr. 22);
23) Specificaţii de preț (anexa nr. 23);
24) Contract – model (anexa nr. 24);
25) Acord adițional (anexa nr. 25);
26) Acord-cadru (anexa nr. 26).

3. Detaliile privind cantitățile de bunuri și servicii, specificațiile tehnice, standardele și resursele sunt prezentate în caietul de sarcini (anexa nr. 21).

4. Autoritatea contractantă urmează să se asigure că la momentul inițierii procedurii de achiziție publică, mijloacele financiare sunt alocate sau există o garanție a alocării lor și destinate exclusiv achiziției în cauză.

5. Atribuirea contractului de achiziție publică de bunuri și servicii se realizează în conformitate cu prevederile Legii nr. 131/2015 privind achizițiile publice.

6. În cazul în care autoritatea contractantă inițiază un acord-cadru, ca modalitate specială de atribuire a contractelor de achiziții publice de bunuri și de servicii, procedura se desfășoară conform Regulamentului cu privire la acordul-cadru ca modalitate specială de atribuire a contractelor de achiziții publice, aprobat prin Hotărârea Guvernului nr. 694/2020.

7. În cazul în care autoritatea contractantă inițiază procedura de negociere, procedura se desfășoară conform Regulamentului cu privire la achizițiile publice folosind procedura de negociere, aprobat prin Hotărârea Guvernului nr. 599/2020.

8. În cazul în care autoritatea contractantă inițiază proceduri cu preselecție se utilizează anexele ce țin de procedurile date: anexa nr. 1, anexa nr. 3, anexa nr. 4, anexa nr. 5, anexa nr. 6 și anexa nr. 25.

9. Ofertantul suportă toate costurile asociate elaborării și prezentării ofertei sale, precum și documentelor care o însoțesc.

10. Cererea de participare (anexa nr. 7), Oferta, Documentul Unic de Achiziții European (în continuare - DUAE), documentația de atribuire, caietul de sarcini şi toată corespondenţa dintre ofertant şi autoritatea contractantă se întocmește în limba română, sau după caz, toate documentele enumerate pot fi întocmite în una din limbile de circulaţie internaţională. Documentele justificative şi literatura de specialitate tipărită, care fac parte din ofertă, pot fi întocmite și în altă limbă, specificată în documentaţia de atribuire, cu condiţia ca acestea să fie însoţite de o traducere exactă a fragmentelor relevante în limba română.

11. În cazul în care autoritatea contractantă a depistat că ofertantul a fost implicat în practicile descrise la pct. 22 și pct. 23 în cadrul procedurii de atribuire pentru contractul de achiziție publică aceasta:

1) exclude ofertantul din procedura respectivă de achiziţie și înaintează solicitarea către Agenția Achiziții Publice privind includerea lui în Lista de interdicție, conform prevederilor Hotărârii Guvernului nr. 1420/2016 pentru aprobarea Regulamentul privind evidenţa Listei operatorilor economici calificaţi; sau

2) întreprinde orice alte măsuri prevăzute în art. 42 al Legii nr. 131/2015 privind achiziţiile publice.

12. Sunt interzise următoarele acţiuni în cadrul procedurii de achiziție:

1) promisiunea sau oferirea unei persoane cu funcție de răspundere, personal sau prin mijlocitor, de bunuri sau servicii, sau privilegii, sau avantaje sub orice formă, pentru a influența acțiunile unei alte părți;

2) orice acțiune sau omisiune, inclusiv interpretare eronată, care, conștient sau din neglijență, induce în eroare sau tinde să inducă în eroare o parte pentru obţinerea unui beneficiu financiar sau de altă natură ori pentru a evita o obligaţie;

3) înţelegerea interzisă de lege, între două sau mai multe părţi, realizată în scopul coordonării comportamentului lor la procedurile de achiziţii publice;

4) prejudicierea, direct sau indirect, a oricărei părţi sau a proprietăţii acestei părţi, pentru a influenţa în mod necorespunzător acţiunile acesteia;

5) distrugerea intenţionată, falsificarea, contrafacerea sau ascunderea materialelor de evidenţă ale investigării, sau prezentarea unor informaţii false organelor de urmărire penală, pentru a împiedica esenţial urmărirea penală condusă de către organele de resort în vederea identificării unor practici frauduloase, precum şi ameninţarea, hărţuirea sau intimidarea oricărei părţi pentru a o împiedica să divulge informaţia cu privire la chestiuni relevante urmăririi penale.

Secţiunea a 2-a

Calificarea candidaților/ofertanților

13. Orice operator economic, rezident sau nerezident, persoana fizică sau juridică de drept public sau privat ori asociație de astfel de persoane are dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii.

14. Persoana fizică sau juridică care a participat la întocmirea documentației de atribuire are dreptul, în calitate de operator economic, de a fi ofertant, ofertant asociat sau subcontractant, dar numai în cazul în care implicarea sa în elaborarea documentației de atribuire nu este de natură să distorsioneze concurența. Persoana fizică sau juridică care participă direct în procesul de verificare şi evaluare a ofertelor nu are dreptul de a fi ofertant, ofertant asociat sau subcontractant, sub sancțiunea excluderii din procedura de atribuire.

15. Mai multe persoane juridice au dreptul să se asocieze în scopul depunerii unei oferte comune, de asemenea, fiecare asociat urmează să prezinte DUAE-ul separat. Asocierea trebuie prezentată în formă scrisă la solicitarea autorității contractante, odată ce a fost declarat în DUAE.

16. Filialele agenților economici, cu personalitate juridică şi înregistrate în conformitate cu prevederile pct. 29, au dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii în nume propriu și, în acest scop, trebuie să prezinte documente care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică și capacitatea economico-financiară.

17. Sucursalele au dreptul de a participa la procedura de atribuire a contractului de achiziţie publică de bunuri și servicii şi de a încheia contractul respectiv numai în numele persoanei juridice, prin împuternicire. În acest caz documentele prezentate, care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică şi capacitatea economico-financiară, trebuie să fie cele ale persoanei juridice.

18. Pentru confirmarea datelor de calificare în cadrul procedurii de achiziții publice, operatorul economic completează și prezintă DUAE, conform formularului standard al Documentului unic de achiziții European, aprobat prin Ordinul ministrului finanțelor nr. 72/2020, în conformitate cu cerințele stabilite de autoritatea contractantă. Prezentarea oricărui alt formular DUAE, este temei de descalificare de la procedura de achiziție publică.

19. În dependență de specificul achiziției și procedura aleasă, autoritatea contractantă are obligația de a stabili pentru fiecare procedură în parte criteriile de calificare cât și documentele suport necesare pentru a fi prezentate de către operatorii economici.

20. Autoritatea contractantă aplică criterii și cerințe de calificare numai referitoare la:

1) eligibilitatea ofertantului sau candidatului;

2) capacitatea de exercitare a activității profesionale;

3) capacitatea economică şi financiară;

4) capacitatea tehnică;

5) standarde de asigurare a calității;

6) standarde de protecție a mediului.

21. Pentru constatarea datelor de calificare în cadrul procedurilor de achiziții publice, operatorul economic prezintă la momentul evaluării documentele solicitate de către autoritatea contractantă în cadrul procedurilor de achiziții publice. Documentele se prezintă în format electronic, utilizînd Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (în continuare - SIA RSAP), cu excepția cazurilor prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

22. Se exclude de la procedura de atribuire a contractului de achiziții publice orice ofertant sau candidat despre care se confirmă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.

23. Se exclude de la procedura pentru atribuire a contractului de achiziţie publică, şi respectiv, nu este eligibil, orice ofertant care se află în oricare dintre situaţiile prevăzute la art. 19 alin. (2) şi alin. (3) și art. 16 alin. (6) al Legii nr. 131/2015 privind achizițiile publice.

24. Orice ofertant/candidat care se află în una din situațiile menționate la pct. 22 și pct. 23 furnizează dovezi care să arate că măsurile luate de el sunt suficiente pentru a demonstra fiabilitatea și credibilitatea sa, în pofida existenței unui motiv de excludere. Dacă autoritatea contractantă consideră astfel de dovezi suficiente, ofertantul/candidatul în cauză nu este exclus de la procedura de achiziție publică, cu excepția cazului în care operatorul economic a fost exclus prin hotărâre definitivă a unei instanțe de judecată de la participarea la procedurile de achiziții publice.

25. Autoritatea contractantă extrage informaţia necesară pentru constatarea existenţei sau inexistenţei circumstanţelor menționate la pct. 22 și pct. 23 în bazele de date disponibile ale autorităţilor publice sau ale părţilor terţe. Dacă acest lucru nu este posibil, autoritatea contractantă are obligaţia de a accepta ca fiind suficient şi relevant pentru demonstrarea faptului că ofertantul/candidatul nu se încadrează în una dintre situaţiile prevăzute la pct. 22 și pct. 23 orice document considerat edificator, din acest punct de vedere, în ţara de origine sau în ţara în care ofertantul este stabilit, cum ar fi certificate, caziere judiciare sau alte documente echivalente emise de autorităţi competente din ţara respectivă.

26. În ceea ce privesc referințele de la pct. 23, în conformitate cu legislaţia internă a statului în care sunt stabiliţi ofertanţii, aceste solicitări se referă la persoanele fizice şi persoanele juridice, inclusiv, după caz, la directori de companii sau la orice persoană cu putere de reprezentare, de decizie ori de control în ceea ce priveşte ofertantul/candidatul.

27. În cazul în care în ţara de origine sau în ţara în care este stabilit ofertantul/candidatul nu se emit documente de natura celor prevăzute la pct. 22 sau respectivele documente nu vizează toate situaţiile referitoare de la pct. 23, autoritatea contractantă are obligaţia de a accepta o declaraţie pe propria răspundere sau, dacă în ţara respectivă nu există prevederi legale referitoare la declaraţia pe propria răspundere, o declaraţie autentică dată în faţa unui notar, a unei autorităţi administrative sau judiciare sau a unei asociaţii profesionale care are competenţe în acest sens.

28. Autoritatea contractantă evaluează măsurile întreprinse de către operatorii economici ținînd seama de gravitatea și circumstanțele particulare ale infracțiunii sau ale abaterii. În cazul în care consideră că măsurile întreprinse sunt insuficiente, autoritatea contractantă informează ofertantul/candidatul despre motivele excluderii.

29. Autoritatea contractantă solicită oricărui ofertant să prezinte dovada din care să rezulte o formă de înregistrare în cazul persoanei juridice, capacitatea legală de a executa documentația de atribuire și de a livra/presta bunurile/serviciile, în conformitate cu prevederile legale din țara în care este stabilit.

30. Ofertantul urmează să dispună de un nivel minim de capacitate economică și/sau financiară și să prezinte informații/documente privind capacitatea economică și/sau financiară pentru a se califica conform cerinţelor de îndeplinire a contractului, cum ar fi:

1) realizarea unei cifre medii anuale de afaceri în ultimii 3 ani egală sau mai mare decât suma stabilită în pct. 16 din anexa nr. 2, care nu trebuie să depășească de două ori valoarea estimată a contractului, cu excepția cazurilor bine justificate, precum cele legate de riscurile speciale aferente naturii bunurilor sau serviciilor;

2) declarații bancare corespunzătoare sau, după caz, dovezi privind asigurarea riscului profesional;

3) situația financiară pentru perioada de gestiune anterioară, avizat și înregistrat de organele competente, și orice alte documente legale edificatoare prin care ofertantul își poate dovedi capacitatea economico-financiară.

31. Atunci când un contract este împărțit pe loturi, indicele cifrei de afaceri se aplică pentru fiecare lot individual. Cu toate acestea, autoritatea contractantă urmează să stabilească cifra de afaceri anuală minimă impusă operatorilor economici cu referire la grupuri de loturi, dacă ofertantului câștigător îi sunt atribuite mai multe loturi care trebuie executate în același timp.

32. La solicitarea autorității contactante, ofertantul urmează să prezinte documentele care demonstrează capacitatea tehnică și/sau profesională pentru executarea viitorului contract numai în măsura în care aceste informaţii sînt relevante pentru îndeplinirea contractului și nu sînt disponibile în bazele de date ale autorităților publice sau ale părților terțe:

1) o listă a principalelor livrări de bunuri/servicii similare efectuate în ultimii 3 ani, conform Anexei nr. 12. Respectivele certificări indică beneficiarii, indiferent dacă aceştia sunt autorităţi contractante sau clienţi privaţi, valorile și perioadele de livrare/prestare.

2) declaraţia referitoare la echipamentele tehnice şi la măsurile aplicate în vederea asigurării calităţii, precum şi, dacă este cazul, la resursele de studiu şi cercetare;

3) informaţii referitoare la personalul/organismul tehnic de specialitate de care dispune sau al cărui angajament de participare a fost obţinut de către ofertant/candidat, în special pentru asigurarea controlului calităţii;

4) certificate sau alte documente emise de organisme abilitate în acest sens, care să ateste conformitatea bunurilor, identificată clar prin referire la specificaţii sau standarde relevante;

5) mostre (în măsura în care necesitatea prezentării este justificată), descrieri şi/sau fotografii a căror autenticitate trebuie să poată fi demonstrată în cazul în care autoritatea contractantă solicită acest lucru;

6) informaţii referitoare la studiile, pregătirea profesională şi calificarea personalului de conducere, precum şi ale persoanelor responsabile pentru îndeplinirea contractului conform Anexei nr. 14;

7) declaraţia referitoare la efectivele medii anuale ale personalului angajat şi ale cadrelor de conducere în ultimii 3 ani;

8) dacă este cazul, informaţii privind măsurile de protecţie a mediului pe care operatorul economic le poate aplica în timpul îndeplinirii contractului de bunuri/servicii, în corespundere cu pct. 36;

9) informaţii referitoare la utilajele, instalaţiile, echipamentele tehnice de care dispune operatorul economic pentru îndeplinirea corespunzătoare al contractului de bunuri/servicii conform Anexei nr. 13;

10) informaţii privind partea din contract pe care operatorul economic are, eventual, intenţia să o subcontracteze, conform Anexei nr. 15. De asemenea, urmează a fi atașat/atașate la Anexa nr. 15, copia/copiile contractului/contractelor încheiat/încheiate cu subatreprenorii.

33. Ofertantul urmează să dispună de un nivel minim de experienţă pentru a se califica conform cerinţelor de îndeplinire a contractului prin demonstrarea experienţei specifice fiind minimum de 3 ani în livrarea/prestarea bunurilor/serviciilor similare, confirmată prin anexarea copiilor contractelor, facturilor și actelor de primire-predare.

34. Operatorul economic urmează să prezinte, în cazul solicitării din partea autorității contactante, documente și certificate emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de asigurare a calităţii (ISO 9001), acestea trebuie să se raporteze la sistemele de asigurare a calităţii, bazate pe seriile de standarde europene relevante, certificate de organisme conforme cu seriile de standarde europene privind certificarea, sau la standarde internaționale pertinente, emise de organisme acreditate.

35. În conformitate cu principiul recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de calitate astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al calităţii.

36. Operatorul economic prezintă documente, certificate, emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de protecţie a mediului, aceasta trebuie să se raporteze:

1) la Sistemul Comunitar de Management de Mediu şi Audit (EMAS), sau;

2) la standarde de gestiune ecologică bazate pe seriile de standarde europene sau internaţionale în domeniu, certificate de organisme conforme cu legislaţia comunitară ori cu standardele europene sau internaţionale privind certificarea.

37. În conformitate cu principiul recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de mediu astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al protecţiei mediului.

38. Autoritățile contractante pot utiliza o serie de criterii generale privind durabilitatea pentru livrarea bunurilor și prestarea serviciilor:

1) Etichetele cu criterii multiple: eticheta europeană (floarea), eticheta scandinavă (lebăda nordică) şi etichetele naţionale (precum îngerul albastru german);

2) Achiziționarea alimentelor organice și cu un aport nutrițional echilibrat pentru școli/gradinițe;

3) Posibilitățile de reciclare/reutilizare a produsului după scoaterea din uz a acestuia;

4) Folosirea de recipiente sau ambalaje reutilizabile pentru transportarea produselor;

5) Furnizarea de hârtie ecologică și reciclată (fără clor și fibră);

6) Restricțiile de utilizare a anumitor substanțe periculoase în compoziția produsului;

7) Sisteme eficiente de tratare a deșeurilor în aer și în apă în fabricarea produselor;

8) Utilizarea sistemelor și schemelor de management de mediu (de exemplu EMAS, ISO 14001);

9) Reducere ale emisiilor de CO2 și a altor gaze prin scăderea frecvenței livrării și opțiuni noi de ambalare;

10) Reciclarea sau reutilizarea ambalajelor care însoțesc produsele;

11) Introducerea specificațiilor pentru vehicole cu cel mai mic nivel posibil de emisii de CO2 pentru categoria și dimensiunile respective, standarde EURO privind emisiile de particule și de Nox;

12) Încurajarea utilizării vehiculelor cu combustibili alternativi și a variantelor electrice sau hibride;

13) Achiziționarea vehiculelor cu sisteme de aer condiționat cu agenți de răcire cu nivel scăzut de GWP (potențial de încălzire globală);

14) Achiziționarea echipamentelor/utilajelor din clasa de eficiență energetică cea mai ridicată;

15) Achiziționarea corpurilor de iluminat cu un conținut scăzut de mercur;

16) Reducerea poluării aerului în orașe (prin achiziția de autobuze și automobile cu nivel scăzut al emisiilor de pulberi în suspensie și oxizi de azot);

17) Achiziționarea de alimente organice și nemijlocit susținerea agriculturii durabile;

18) Economisirea resurselor naturale (prin achiziția de produse obținute din materiale reciclate, reducerea consumului de hârtie prin achiziționarea, promovarea utilizării dispozitivelor multifuncționale);

19) Achziționarea de materiale de construcție și aprovizionare durabilă;

20) Încurajarea utilizării de materiale reciclate în construcție;

21) Aprovizionarea cu produse certificate ca fiind durabile (Patru etichete ecologice ale UE pentru componente);

22) Achiziționarea și utilizarea de materiale de construcție cu impact redus asupra mediului;

23) Serviciile pentru depozitarea deșeurilor reciclabile și sistemul de gestionare a deșeurilor;

24) Gestionarea deșeurilor din demolări;

25) Achiziționarea serviciilor de curăţenie ecologică folosind produse care întrunesc cerințele etichetelor ecologice;

26) Achiziționarea serviciilor de catering cu alimente ecologice (bio), indicînd procentul de alimente ecologice;

27) Utilizarea unui sistem de management de mediu (EMS) pentru servicii de catering;

28) Utilizarea de metode non-chimice, care respectă mediul;

29) Achiziționarea de energie electrică ecologică;

30) Impunerea unor durate de viață prelungite ale produselor și a unei garanții pentru piesele de schimb;

31) și altele.

39. În cazul unei asocieri, cerințele solicitate pentru îndeplinirea criteriilor de calificare și de selecție referitoare la situația economică și financiară sau a capacităților tehnice și profesionale pot fi îndeplinite prin cumul proporțional sarcinilor ce le revin fiecărui asociat.

40. În ceea ce privește criteriile privind cifra de afaceri, în cazul unei asocieri, cifra de afaceri medie anuală luată în considerare este valoarea generală, rezultată prin însumarea cifrelor de afaceri medii anuale corespunzătoare fiecărui membru al asocierii.

41. În ceea ce priveşte experienţa, pentru a se califica conform cerinţelor stabilite, asociațiile trebuie să demonstreze o experiență proporțională sarcinilor ce revin fiecărui asociat.

42. Capacitatea economică şi financiară, cât și capacitatea tehnică şi/sau profesională a ofertantului/candidatului poate fi susţinută, pentru îndeplinirea unui contract, şi de o altă persoană, indiferent de natura relaţiilor juridice existente între ofertant/candidat şi persoana respectivă.

43. În cazul în care ofertantul/candidatul îşi demonstrează capacitatea economică şi financiară cât și capacitatea tehnică şi/sau profesională invocînd şi susţinerea acordată, în conformitate cu prevederile pct. 42 de către o altă persoană, acesta are obligaţia de a dovedi susţinerea de care beneficiază prin prezentarea în formă scrisă a unui angajament ferm al persoanei respective, încheiat în formă autentică (conform anexelor nr. 16 și nr. 18) şi declaraţiile terţului susţinător financiar şi terţului susţinător tehnic și profesional (anexele nr. 17, nr. 19 şi nr. 20), prin care această persoană confirmă faptul că pune la dispoziţia ofertantului/candidatului resursele financiare cât și resurse tehnice și profesionale invocate. Prezentarea angajamentului se face la solicitarea autorității contractante odată ce a fost declarat în DUAE. Persoana care asigură susţinerea financiară cât și tehnică și profesională trebuie să îndeplinească criteriile de selecție relevante și nu trebuie să se afle în niciuna dintre situaţiile prevăzute la pct. 22 și pct. 23 care determină excluderea din procedura de atribuire.

Secţiunea a 3-a

Pregătirea/Elaborarea ofertelor

44. Autoritatea contractantă în caietul de sarcini descrie condițiile/cerințele de furnizare:

a) ***a energiei electrice,*** în conformitate cu Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare adoptate de către Consiliul de administrație al Agenției Naţionale pentru Reglementare în Energetică (în continuare – ANRE), de exemplu: Regulamentul privind furnizarea energiei electrice, aprobat prin Hotărârea ANRE nr. 23/2017, Regulamentul privind racordarea la rețele electrice și prestarea serviciilor de transport și de distribuție a energiei electrice, aprobat prin Hotărârea ANRE nr. 168/2019, Metodologia de calculare, aprobare și aplicare a tarifelor reglementate pentru serviciile auxiliare prestate de operatorii de sistem din sectorul electroenergetic, aprobată prin Hotărârea ANRE nr. 269/2018, Instrucțiunea privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007, Instrucţiunea privind calcularea consumului tehnologic de energie electrică în reţelele de distribuţie, în funcţie de valoarea factorului de putere în instalaţiile de utilizare, aprobată prin Hotărârea ANRE nr. 89/2003 etc.

b) a gazelor naturale în conformitate cu Legea nr. 108/2016 cu privire la gazele naturale și Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea gazelor naturale, aprobat prin Hotărârea ANRE nr. 113/2019.

c) a energiei termice în conformitate cu Legea nr. 92/2014 cu privire la energia termică și promovarea cogenerării și Legea nr. 174/2017 cu privire la energetică, și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea energiei termice, aprobat prin Hotărârea ANRE nr. 169/2019.

d) a alimentării cu apă şi canalizare în conformitate cu Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare și actele normative secundare, de exemplu: Regulamentul-cadru de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare, aprobat prin Hotărârea ANRE nr. 355/2019 sau Regulamentele de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare aprobate de autoritățile publice locale de nivelul întâi, în cazul în care au fost elaborate și aprobate.

e) ***a produselor petroliere pentru alimentarea automobilelor*** conform listei complete privind rețeaua de distribuție la nivelul țării din care să rezulte ca ofertantul deține stații de alimentare în localitățile indicate în documetația de atribuire. Carburantul se livrează la stația de alimentare în baza cardurilor emise de către Furnizor. Ofertantul oferă autorității contractante posibilitatea de a achiziționa carburant (fără plată în numerar) prin intermediul cardurilor valorice la stațiile de alimentare ale furnizorului la nivelul fiecăreia dintre localitățile menționate în documetația de atribuire. În cazul în care locul destinației finale îl constituie mai multe localități/regiuni, atribuirea contractelor de achiziție se realizează pe loturi pentru fiecare localitate/regiune în parte. Livrarea cardurilor se face pe baza unei cereri de emitere de card din partea autorității contractante. Termenul solicitat pentru livrarea cardurilor la sediul autorităţii contractante este de 5 zile lucrătoare de la data intrării în vigoare a contractului şi, respectiv, de la data transmiterii cererii de emitere de carduri suplimentare.

45. Autoritatea contractantă în caietul de sarcini precizează detalii privind modul de transportare, prestare, utilizare a produselor/serviciilor:

a) produselor petroliere pentru alimentarea automobilelor

Furnizorul acordă permanent achizitorului posibilitatea accesării on-line a informaţiilor privind situaţia detaliată a tuturor achiziţiilor de carburant efectuate de către fiecare autovehicul al său. Posibilitatea achizitorului de a obţine la orice staţie de distribuţie pe bază de card, informaţii privind valoarea rămasă pentru fiecare card în parte. Furnizorul gestionează lista cardurilor pierdute sau furate şi are obligaţia să blocheze/deblocheze utilizarea acestora în cel mult 24 ore de la solicitarea achizitorului. Furnizorul are obligația de a garanta că produsele furnizate respectă standardele minime de poluare aprobate conform legislației naționale și pot fi alimentate de la stațiile existente în localitățile indicate în documetația de atribuire. Carburanţii livraţi trebuie să corespundă calitativ normelor în vigoare. Se prezintă în partea II, Condițiile Speciale a Contractului, cât și în anexa nr.1 la Contract „Specificaţii Tehnice”, condiţiile

tehnice de calitate şi metodele de determinare a produselor, având la bază standarde şi omologări naţionale sau internaţionale. Furnizorul asigură personalizarea cardurilor pe fiecare autovehicul (pe număr de înmatriculare), configurarea cardului pe tipul carburantului. Furnizorul asigură asistență permanentă 24 h, 7 zile din săptămână, pentru ca, în cazul apariției anumitor deficiențe în funcționarea cardurilor pentru carburant, Furnizorul să fie în măsură să soluționeze problemele apărute în cel mai scurt timp posibil. Furnizorul specifică dacă toate cardurile sunt acceptate la toate stațiile PECO situate în localitățile menționate în documentația de atribuire. Furnizorul pune la dispoziţia achizitorului instrucţiuni de folosire a cardului. Autoritatea contractantă își rezervă dreptul de a mări sau micșora numărul de carduri și de a suplimenta sau diminua cantitatea de carburanți în baza prevederilor normative.

b) ***de furnizare a energiei electrice***

Evidența consumului de energie electrică se efectuează prin intermediul echipamentului de măsurare al Beneficiarului care este responsabil de integritatea acestuia. În cazul în care echipamentul de măsurare este instalat în limitele proprietății operatorului de sistem, responsabil de integritatea echipamentului de măsurare și a sigiliilor aplicate este operatorul de sistem. Operatorul de sistem asigură, la solicitare, accesul Beneficiarului la echipamentul de măsurare. În acest caz, Beneficiarul este în drept să aplice sigiliul său echipamentului de măsurare. Lucrările de instalare, exploatare, deservire, reparare, verificare metrologică periodică și de înlocuire a echipamentului de măsurare al Beneficiarului se efectuează în conformitate cu Legea nr. 174/2017 cu privire la energetică și Legea nr. 107/2016 cu privire la energia electrică, iar cheltuielile se suportă de către Beneficiar. Controlul echipamentului de măsurare și al sigiliilor aplicate acestuia se efectuează de către operatorul de sistem, după necesitate, și numai în prezența reprezentantului Beneficiarului. Citirea indicilor echipamentului de măsurare în scopul facturării energiei electrice consumate de Beneficiar, se efectuează de operatorul de sistem lunar. Personalul operatorului de sistem și utilizatorul de sistem sunt în drept să stabilească, de comun acord, timpul efectuării activităților pentru citirea indicilor echipamentului de măsurare. Cantitatea energiei electrice furnizate Beneficiarului se determină în baza indicilor echipamentului de măsurare, citite la fiecare loc de consum, sau, în cazurile prevăzute în Regulamentul pentru furnizarea energiei electrice, se calculează prin estimare. În cazul deteriorării echipamentului de măsurare sau dacă se constată încălcarea de către Beneficiar a prevederilor Legii cu privire la energia electrică, care a dus la consum de energie electrică prin evitarea echipamentului de măsurare, prin denaturarea indicațiilor echipamentului de măsurare sau alte modalități de consum neînregistrat de echipamentul de măsurare, contravaloarea energiei electrice consumate se calculează în conformitate cu prevederile Regulamentului pentru furnizarea energiei electrice. Contravaloarea pierderilor de energie electrică în transformatoarele de forță și în liniile electrice ce aparțin Beneficiarului, se calculează în baza Instrucțiunii privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007.

46. Autoritatea contractantă în caietul de sarcini precizează modalitatea de calculare a costului/prețului bunului/serviciului, prin trimitere la actele normative din domeniu.

a) a produselor petroliere pentru alimentarea automobilelor

Prețul unui litru de carburant ofertat va fi cel afișat la stațiile de alimentare ale ofertantului cu aplicarea discount-ului ofertat.

Furnizorul asigură autorității contractante posibilitatea de a stabili limite individuale valorice pentru fiecare card, inclusiv de a le modifica în sensul majorării sau micșorării acestora. Prețul unitar ofertat constituie prețul mediu calculat de către ofertant utilizînd prețurile afișate la panourile informative în toate stațiile din localitate/regiune indicate în documentația de atribuire, în decurs de 15 zile până la data publicării anunțului de participare în Buletinul achizițiilor publice, la care se aplică un discount.

Calcularea prețului unitar se efectuează conform formulei:

$$\mathrm{Pu} = \frac{(\mathrm{M1} + \mathrm{M2} + \cdots + \mathrm{M15})}{15} - D\%$$

Unde,

Pu – reprezintă prețul unitar ofertat;

M_1–reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru prima zi;

M_2– reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a doua zi;

M_{15}– reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a cincisprezecea zi;

D% –reprezintă discount-ul aplicat.

Discount-ul este specificat expres în ofertă și ulterior în anexa nr. 2 la contract, rămânînd neschimbat pe întreaga perioadă de valabilitate al acestuia. Propunerea financiară este însoțită obligatoriu de documentele confirmative cu privire la prețurile prezentate (bon fiscal). Furnizorul facturează contravaloarea produselor la sfârșitul fiecărei luni, pentru consumul efectuat, conform unei centralizări cu cantitatea alimentată pe fiecare autovehicul în parte. Factura aferentă consumului înregistrat pe fiecare card în parte este însoțită de un raport de consum care conține informații detaliate cu privire la tranzacțiile efectuate pe fiecare card și mașină, locație, dată, ora alimentării, tipul carburantului și, după caz, subtotalul cardului și totalul general de carburant după fiecare tranzacție.

În cazul procurării produselor petroliere pentru alimentarea automobilelor, în conformitate cu art. 26 al Legii nr.131/2015 privind achizițiile publice, se aplică criteriul cel mai bun raport calitate-preț, din care factorul de evaluare prețul, constituie minimum 60%, iar restul factorilor sunt la decizia autorității contractante (ex: discount-ul, amplasarea stațiilor PECO, etc.).

În restul cazurilor ce ține de achiziționarea de carburanţi lichizi şi/sau gazoşi în vrac, uleiuri, etc. se utilizează principiul general de procurare a bunurilor.

b) ***a energiei electrice***

Consumul tehnologic de energie electrică, cauzat de factorul de putere din instalaţiile electrice ale Beneficiarului se facturează numai în cazul în care factorul de putere Cos φ, calculat în punctul de delimitare, este mai mic de _____(0,92 pentru instalația de utilizare racordată la tensiunea 0,4 kV și 0,87 la tensiunea 10(6) kV). Cantitatea consumului tehnologic de energie electrică, cauzat de factorul de putere din instalaţiile electrice ale Beneficiarului se calculează în baza Instrucţiunii privind calcularea consumului tehnologic de energie electrică în reţelele de distribuţie, în funcţie de valoarea factorului de putere în instalaţiile de utilizare, aprobată prin Hotărârea Consiliului de administraţie al Agenţiei nr.89 din 13/2003. În cazul în care furnizorul calculează prețul reieșind din tariful ANRE minus – discount-ul, modul de calculare a prețului se indică în condițiile speciale a contractului și de asemenea se indică și cazurile de modificare a lui. Micșorarea și/sau majorarea prețului și valorii contractului se efectuează prin acord adițional la contract.

47. Operatorul economic interesat de a participa la procedura de achiziție publică este obligat să depună până la expirarea termenului-limită stabilit de către autoritatea contractantă, în acest sens, o cerere de participare, în cazul aplicării prevederilor art. 33 alin. (7) și alin. (11) al Legii nr. 131/2015. În celelalte cazuri, aceasta se depune odată cu oferta.

48. Oferta cuprinde următoarele formulare:

1) Propunerea tehnică - ofertantul elaborează propunerea tehnică, astfel încât aceasta să respecte în totalitate cerinţele de calificare, precum şi cerinţele prevăzute în caietul de sarcini. Propunerea tehnică conține -Specificaţii tehnice (anexa nr. 22);

2) Propunerea financiară- ofertantul elaborează propunerea financiară, astfel încât aceasta să furnizeze toate informaţiile solicitate cu privire la preţuri, tarife, precum şi la alte condiţii financiare şi

comerciale legate de obiectul contractului de achiziţie publică de bunuri și servicii. Propunerea financiară conține - Specificații de preț (anexa nr.23);

3) DUAE;

4) Garanția pentru ofertă, după caz (anexa nr.9).

49. Toate documentele menţionate la pct. 48 se completează fără nici o modificare sau abatere de la formulare, spaţiile goale fiind completate cu informaţia solicitată. Completarea defectuoasă a formularelor atrage respingerea ofertei.

50. Operatorii economici pregătesc ofertele conform cerințelor stabilite în anunțul de participare, publicat de către autoritatea contractantă în Buletinul achizițiilor publice, și depun ofertele în mod electronic, folosind fluxurile interactive de lucru puse la dispoziție de platformele electronice, cu excepția cazurilor prevăzute la art. 33 alin. (7) şi alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

51. Ofertantul depune garanția pentru ofertă conform prevederilor Legii nr. 131/2015 privind achizițiile publice.

52. În cazul unei asocieri, garanția pentru ofertă se depune de liderul asociației.

53. Ofertantul are obligația, prin depunerea declarației privind valabilitatea ofertei (anexa nr. 8), de a menține oferta valabilă pe toată perioada de valabilitate prevăzută în documentația de atribuire. Termenul valabilităţii ofertei începe să decurgă din momentul termenului limită de depunere a ofertelor. Orice ofertă valabilă pentru o perioadă mai mică decât cea prevăzută în anexa nr. 2 se respinge de către grupul de lucru ca fiind necorespunzătoare.

54. În cazul extinderii perioadei de valabilitate a ofertei, perioada de valabilitate a garanției pentru ofertă se prelungește în mod corespunzător.

55. Ofertantul are obligația de a comunica autorității contractante dacă este sau nu este de acord cu prelungirea perioadei de valabilitate a ofertei. Ofertantul care nu este de acord cu prelungirea perioadei de valabilitate a ofertei se consideră că și-a retras oferta, fără ca acest fapt să atragă pierderea garanției pentru ofertă.

56. Ofertele care conţin o perioadă de garanţie mai mică decât perioada de valabilitate a ofertelor prevăzută în anexa nr. 2 se resping de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice.

57. Autoritatea contractantă stabileşte perioada maximă de livrare/prestare a bunurilor/serviciilor în anexa nr. 2.

58. Preţurile pentru bunurile/serviciile solicitate se indică în lei moldoveneşti, cu două cifre după virgulă, cu excepţia cazurilor în care anexa nr. 2 prevede altfel.

Secţiunea a 4-a

Depunerea și deschiderea ofertelor

59. Oferta scrisă şi semnată în format electronic, de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită atât și în cazul delegării sau împuternicirii persoanei, la ofertă se anexează actul/documentul de împuternicire și se prezintă conform cerinţelor expuse în anexa nr. 2 în conformitate cu instrumentele existente în SIA RSAP, cu excepția cazurilor prevăzute la art. 33 alin. (7) şi alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

60. Ofertantul trebuie să ia toate măsurile, astfel încât oferta să fie recepționată și înregistrată în SIA RSAP până la data limită pentru depunerea ofertelor, ținând cont de timpul necesar pentru încărcarea ofertei în sistem. În cazul prezentării ofertelor pe suport de hârtie, autoritatea contractantă eliberează operatorului economic, în mod obligatoriu, o recipisă în care indică data și ora recepționării ofertei.

61. Documentele justificative în sprijinul informațiilor declarate în DUAE, care conțin date cu caracter personal, se prezintă separat, pe suport de hârtie sau în formă scanată, cu aplicarea semnăturii electronice, utilizînd mijloace electronice de comunicare sau alte mijloace la etapa evaluării ofertelor, la solicitarea autorității contractante.

62. SIA RSAP nu acceptă ofertele transmise după expirarea termenului limită de depunere a ofertelor.

63. În cazurile prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice, ofertele depuse după termenul limită de deschidere a ofertelor se înregistrează de către autoritatea contractantă și se restituite ofertantului, fără a fi deschise.

64. În cazul asocierii conform pct. 15, fiecare dintre aceştia îşi asumă obligaţia pentru oferta comună şi răspunde pentru orice consecinţe ale viitorului contract de achiziţie publică. Informaţia privind asocierea se prezintă completînd anexa nr. 11.

65. Ofertantul nu are dreptul de a depune decât o singură ofertă de bază. Ofertanţii asociaţi nu au dreptul de a depune alte oferte, în mod individual, pe lângă oferta comună. Ofertele alternative se depun numai dacă autoritatea contractantă a precizat explicit în anunţul de participare că permite sau solicită depunerea de oferte alternative.

66. Persoanele juridice nominalizate ca subcontractanţi în cadrul uneia sau mai multor oferte nu au dreptul de a depune oferta în nume propriu sau în asociere.

67. Ofertantul are dreptul să modifice sau să retragă oferta înainte de expirarea termenului de depunere a ofertelor, fără a pierde dreptul de retragere a garanţiei pentru ofertă.

Secţiunea a 5-a

Evaluarea și compararea ofertelor

68. În cazul în care ofertele conțin secrete tehnice, comerciale sau țin de protecția proprietății intelectuale, autoritatea contractantă asigură păstrarea confidenţialităţii asupra conţinutului ofertei, precum şi asupra oricărei informaţii privind ofertantul și totodată, asigura dreptul operatorului economic de a nu face publice aceste date prin aplicarea art. 33 alin. (7) și alin. (11) al Legii nr. 131/2015 privind achizițiile publice, însă aplicarea acestui articol se referă numai la partea ce conțin datele enumeratate mai sus.

69. Examinarea documentelor de către autoritatea contractantă se efectuează în baza informațiilor prezentate de către operatorii economici în DUAE, și conform cerințelor stipulate în anunțul de participare prin care menționează că:

1) este eligibil să participe la procedurile de achiziții publice și nu există motive de excludere din cadrul procedurilor de achiziții publice pentru atribuirea contractului de achiziție publică;

2) îndeplinește criteriile referitoare la situația economică și financiară și/sau capacitatea tehnică și profesională stabilite de autoritatea contractantă în anunțul de participare sau în documentația de atribuire.

3) se obligă să asigure și să respecte standardele de asigurare a calităţii și standardele de protecţie a mediului.

70. DUAE a operatorilor economici se verifică după caz, direct de către autoritatea contractantă prin procedurile automate desfășurate în SIA RSAP, prin accesarea unei baze de date a autorităților publice sau a terților din Republica Moldova, iar atunci când este necesar și în alte state.

71. În cazul în care la evaluare se stabilesc discrepanțe între informațiile prezentate de către operatorul economic în DUAE și cerințele stabilite de către autoritatea contractantă, operatorul economic se descalifică, ceea ce duce la respingerea ofertei, fiind stabilită ca inacceptabilă și neconformă, și se examinează documentele următorului ofertant/candidat.

72. Operatorul economic a cărui informație prezentată în DUAE corespunde cerințelor/condițiilor specificate de către autoritatea contractantă în anunț/invitația de participare are obligația să prezinte la cerere și fără întârziere documentele justificative.

73. Ofertantul clasat pe primul loc după aplicarea criteriului de atribuire prezintă documentele justificative prin care să demonstreze că îndeplineşte în totalitate cerinţele corespunzătoare criteriilor de calificare și de selecție, în conformitate cu informaţiile cuprinse în DUAE, cu excepţia procedurilor desfăşurate în mai multe etape, când documentele justificative sunt solicitate înainte de transmiterea invitaţiilor pentru etapa a doua către candidaţii selectaţi.

74. Ofertele se examinează de către grupul de lucru creat de autoritatea contractantă sau, după caz, specialistul certificat în domeniul achizițiilor publice.

75. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice are obligaţia de a stabili care sunt clarificările necesare pentru evaluarea fiecărei oferte, precum şi perioada acordată pentru transmiterea clarificărilor.

76. În cazul unei oferte care are un preț anormal de scăzut în raport cu prețul estimat al achiziției, autoritatea contractantă are obligația de a efectua controlul calculării elementelor prețului și de a verifica și anumite elemente ale propunerii financiare stabilite ca fiind cu preț anormal de scăzut cât și respectarea de către ofertant a cerințelor tehnice indicate în caietul de sarcini, și de a solicita în scris, și înainte de a lua o decizie de respingere a acelei oferte, detalii și precizări pe care le consideră relevante cu privire la ofertă, precum, și de a verifica răspunsurile care justifică prețul respectiv.

77. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice respinge oferta în oricare dintre următoarele cazuri:

1) ofertantul nu îndeplinește cerințele de calificare și de selecție;

2) oferta nu respectă cerinţele prevăzute în documentaţia de atribuire pentru elaborarea şi prezentarea ofertelor;

3) ofertantul nu transmite în perioada stabilită clarificările solicitate;

4) oferta financiară nu are un preț fixat;

5) ofertantul modifică, prin clarificările pe care le prezintă, conţinutul propunerii tehnice şi/sau al propunerii financiare, cu excepţia situaţiei în care modificarea este determinată de corectarea erorilor aritmetice sau abaterilor neînsemnate;

6) oferta este anormal de scăzută potrivit art. 70 al Legii nr. 131/2015 privind achizițiile publice;

7) atunci când explicațiile prezentate de ofertant, la solicitarea autorității contractante, nu sunt concludente şi/sau nu sunt susținute de documentele justificative cerute de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice;

8) s-a constatat comiterea unor acte de corupţie, acte conexe actelor de corupţie sau fapte coruptibile confirmate prin hotărâre definitivă a instanţei de judecată.

78. Dacă oferta, inclusiv formularele care o însoțesc, nu corespunde cerințelor prestabilite în invitația/anunțul de participare, inclusiv în documentația de atribuire sau aceasta nu este completată, semnată electronic și după caz, semnată și ștampilată în modul corespunzător, ea se respinge de către autoritatea contractantă, și nu poate fi rectificată cu scopul de a corespunde cerințelor, prin corectarea

sau extragerea devierilor sau rezervelor necorespunzătoare, excepție constituind doar corectarea greșelilor aritmetice sau abaterilor neînsemnate.

79. Autoritatea contractantă poate, la discreţia sa, să ceară oricăruia dintre ofertanţi o clarificare a ofertei acestora, pentru a facilita examinarea, evaluarea și compararea ofertelor. Nu se solicită, nici nu se permit schimbări în preţurile sau în conţinutul ofertei, cu excepţia corectării erorilor aritmetice descoperite de către autoritatea contractantă în timpul evaluării ofertelor.

80. Erorile aritmetice se corectează după cum urmează: dacă există o discrepanţă între preţul pentru o unitate de măsură şi preţul total (care este obţinut prin multiplicarea preţului cu cantitatea totală), se ia în considerare preţul pe unitate, iar preţul total este corectat în mod corespunzător.

81. Grupul de lucru, după caz, specialistul certificat în domeniul achizițiilor publice are dreptul de a corecta erorile aritmetice numai cu acceptul ofertantului. Dacă ofertantul nu acceptă corectarea acestor erori, oferta sa se consideră necorespunzătoare şi, în consecinţă, se respinge de către grupul de lucru.

82. Operatorul economic este obligat să răspundă la solicitarea de clarificare a autorității contractante în cel mult 3 zile lucrătoare sau, în cazul în care procedura folosită este cererea ofertelor de preţuri, cel mult o zi lucrătoare de la data expedierii acesteia, iar în cazul în care ofertantul nu suplimentează, nu prezintă clarificări sau nu completează informațiile sau documentele solicitate de autoritatea contractantă în termenele stabilite de aceasta, oferta se respinge şi se selectează următoarea după clasament dintre ofertele rămase în vigoare.

83. Oferta care corespunde tuturor termenilor, condiţiilor şi specificaţiilor din documentele de atribuire, fără abateri esenţiale sau cu abateri neînsemnate, erori sau omiteri ce pot fi înlăturate fără a afecta esenţa ei, se consideră conformă.

84. Autoritatea contractantă descalifică ofertantul care depune documente ce conţin informaţii false, cu scopul calificării, sau derutează ori face reprezentări neadevărate pentru a demonstra corespunderea sa cerinţelor de calificare. În cazul în care acest lucru este dovedit, autoritatea contractantă declară ofertantul respectiv ca fiind neeligibil pentru participarea ulterioară în contractele de achiziţii publice, în urma includerii lui în Lista de interdicţie a operatorilor economici.

85. Autoritatea contractantă solicită ofertanţilor să demonstreze împuternicirea de a încheia contractele de achiziţii publice şi componenţa fondatorilor, asociațiilor, acționarilor, administratorilor și a beneficiarilor efectivi.

86. Ofertantul/ofertantul asociat desemnat câștigător este obligat de a completa și prezenta declarația cu privire la beneficiarii efectivi în conformitate cu Ordinul ministrului finanțelor nr. 145/2020 cu privire la aprobarea Declarației privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani.

Secţiunea a 6-a

Atribuirea contractului

87. Autoritatea contractantă anulează procedura de atribuire a contractului de achiziţie publică conform art. 71 din Legea nr. 131/2015 privind achizițiile publice.

88. Decizia de anulare nu creează vreo obligaţie a autorității contractante față de ofertanţi, cu excepţia returnării garanţiei pentru ofertă. Decizia de anulare a procedurii de atribuire se expediază Agenției Achiziții Publice nu mai târziu de data informării despre rezultatele procedurii de atribuire prevăzută la art. 31 alin. (1) al Legii nr. 131/2015 privind achizițiile publice.

89. În cazul în care se anulează aplicarea procedurii pentru atribuirea contractului de achiziţie publică, autoritatea contractantă are obligaţia de a comunica în scris tuturor participanţilor la procedura de achiziţie publică, în cel mult 3 zile de la data anulării procedurii, atât încetarea obligaţiilor pe care aceştia şi le-au creat prin depunerea de oferte, cât şi motivul anulării.

90. Darea de seamă privind anularea procedurii de achiziţie publică este întocmită de către autoritatea contractantă şi este publicată în Buletinul achizițiilor publice nu mai târziu de data emiterii deciziei de anulare a procedurii de achiziţie publică.

91. La momentul încheierii contractului, dar nu mai târziu de data expirării garanţiei pentru ofertă, după caz, ofertantul câştigător prezintă garanţia de bună execuţie, în conformitate cu cerințele stipulate în art. 68 al Legii nr. 131/2015 privind achizițiile publice.

92. Garanția de bună execuție a contractului, dacă părțile agreează, se constituie din:

1) reţineri succesive din plata cuvenită pentru facturile fiscale înaintate, cu efectuarea transferului sumei respective pe un cont special deschis de către operatorul economic, pus la dispoziția autorității contractante, la o bancă licențiată, agreată de ambele părți;

2) reţineri succesive directe din plata cuvenită pentru facturile fiscale înaintate;

3) transfer pe contul autorității contractante;

4) formă de garanţie bancară de la o instituţie licenţiată, (anexa nr.10).

93. Refuzul ofertantului câştigător de a depune garanţia de bună execuţie sau de a semna contractul constituie motiv pentru anularea atribuirii contractului şi reţinerii garanţiei pentru ofertă. În acest caz, autoritatea contractantă poate atribui contractul următorului ofertant cu oferta cea mai bine clasată, a cărui ofertă este conformă cerinţelor şi care este apreciată de către autoritatea contractantă a fi calificată în executarea contractului. Totodată, autoritatea contractantă este în drept să respingă toate celelalte oferte.

94. La expirarea perioadei de așteptare sau, după caz, după soluționarea oricăror contestații, sau monitorizării conformităţii desfăşurării procedurilor de achiziţii publice de către Agenția Achiziții Publice, autoritatea contractantă încheie contractul de achiziții publice, în conformitate cu termenii și condițiile indicate în documentația de atribuire.

95. La data încheierii contractului de achiziție publică de bunuri/servicii se interzice modificarea unor elemente ale ofertei câștigătoare, impunerea de noi cerințe ofertantului câștigător sau implicarea oricărui alt ofertant decât cel care a prezentat oferta cea mai avantajoasă.

96. Contractul pentru care sursele financiare se alocă din bugetul de stat/bugetul local se înregistrează obligatoriu la una din trezoreriile regionale ale Ministerului Finanțelor și intră în vigoare la data înregistrării sau la o altă dată ulterioară prevăzută de acesta după înregistrare la una din trezoreriile regionale ale Ministerului Finanțelor.

97. Autoritatea contractantă utilizează contractul - model (anexa nr. 24) din prezenta documentație-standard, inclusiv pentru contracte subsecvente încheiate conform acordului-cadru (anexa nr. 26), pentru contracte de valoare mică, pentru contractele în urma desfășurării procedurii prin cererea ofertelor de prețuri, la fel și pentru contractele în urma desfășurării procedurilor negociate. Contractul poate fi încheiat între una sau mai multe autorități contractante și unul sau mai mulți operatori economici, care are ca obiect livrarea/prestarea bunurilor/serviciilor.

98. Contractul este compus din două părți: Partea I cea generală care este obligatorie, și care nu se modifică, doar cu excepția contractelor de achiziții publice ce nu cad sub incidența Legii nr. 131/2015 privind achiziţiile publice și Partea II ceea ce ține de condițiile speciale al contractului care se completează doar la necesitate, unde autoritatea contractantă are dreptul de a stabili condiții/cerințe speciale în dependență de obiectul achiziției, de complexitatea procedurii, atât și de a stabili condițiile achitării (în special la achiziționarea combustibilului, energiei electrice, gaze, apa și canalizare, salubritate, servicii de comunicații electronice, etc.), atât și de a stabili condițiile achitării în avans. În cazul achizițiilor serviciilor din domeniul energetic și de alimentare cu apă și de canalizare, contractul

de achiziții publice conțin clauzele obligatorii stabilite prin legile sectoriale și actele normative de reglementare aprobate de către ANRE. Totodată, prevederile obligatorii stabilite prin deciziile acesteia, care nu se regăsec în partea I cea generală al contractului, se indică în partea II ce ține de condițiile speciale al contractului.

99. Termenii de asumare a angajamentelor în contractele de achiziții publice de către autoritățile/instituțiile bugetare se stabilesc în conformitate cu prevederile art. 66 din Legea nr. 181/2015 finanțelor publice și responsabilității bugetar-fiscale.

100. În cazul serviciilor de audit, autoritatea contractantă indică în partea II ce ține de condițiile speciale al contractului drepturile/obligațiile Beneficiarului și drepturile/obligațiile Prestatorului, în conformitate cu prevederile Ordinului ministrului finanțelor nr. 160/2020 cu privire la aprobarea Regulamentului privind activitatea de audit intern pe bază de contract în sectorul public.

101. Nu se acceptă în cadrul achizițiilor publice proiectele contractelor ce deviază de la anexa nr. 24, întocmite de prestator/furnizor cu excepția cazurilor când serviciile sunt prestate în afara țării și sunt încheiate conform cadrului juridic local (de exemplu: serviciile de instruire, servicii hoteliere, etc.).

102. Orice operator economic care consideră că, în cadrul procedurilor de achiziţie, autoritatea contractantă, prin decizia emisă sau prin procedura de achiziţie aplicată cu încălcarea legii, a lezat un drept al său recunoscut de lege, în urma cărui fapt el a suportat sau poate suporta prejudicii, are dreptul să conteste decizia sau procedura aplicată de autoritatea contractantă, în modul stabilit de Legea nr. 131/2015 privind achiziţiile publice.

103. Contestaţiile se depun direct la Agenția Națională pentru Soluționare a Contestațiilor. Toate contestaţiile se depun, se examinează şi se soluţionează în modul stabilit de Legea nr. 131/2015 privind achiziţiile publice.

104. Operatorul economic, conform art. 83 al Legii nr. 131/2015 privind achizițiile publice, în termen de până la 5 zile, sau10 zile de la data la care a aflat despre circumstanţele ce au servit drept temei pentru contestaţie, are dreptul să depună la Agenţia Națională pentru Soluționarea Contestațiilor o contestaţie argumentată a acţiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

105. Contestaţiile privind anunțurile de participare la licitaţie şi documentaţia de atribuire se depun în termenele indicate la pct. 104, însă nu mai târziu de deschiderea ofertelor de către autoritatea contractantă.

106. Fiecare ofertant care participă, în mod individual sau ca asociat, la procedura de atribuire a contractului de achiziţie publică de bunuri/servicii are obligația să prezinte anexele prevăzute în prezenta documentație, completate în mod corespunzător şi semnate de persoanele autorizate, conform cerințelor stabilite în anexa nr.2.

Anexa nr. 2
la Documentația standard nr._____
din "____" _____ 20___

ANUNȚ DE PARTICIPARE INCLUSIV PENTRU PROCEDURILE DE PRESELECȚIE/PROCEDURILE NEGOCIATE

privind achiziționarea: ***Echipament pentru asigurarea funcționării rețelei corporative***

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/lib.php?l=ro&idc=532&t=/Achizitii-publice/Plan-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; 022-257-752 .*
5. **Adresa de e-mail şi pagina web oficială ale autorității contractante:** achizitiicnas@cnas.gov.md , www.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.*
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: **32420000-3**

Specificația tehnică

Specificarea tehnică deplină solicitată, Standarde de referinţă			**Cantitatea**	**Valoarea estimată fără TVA lei MLD**	**Pasul minim de licitare (electronică) lei MLD**
Lotul 1. *Router*					
Lotul 1. *Router*	Type	Router **CISCO C8300-1N1S-6T care va permite funcționarea în regim standby**	**1 bucăți**	**150 000,00**	**1 500,00**
	Rack Units (RU)	**1RU**			
	Memory (DRAM) default	**8 GB**			
	Storage	**16 GB**			

	(M.2 SSD)				
	Flash memory support	**8 G**			
	Interface	**1x1G WAN (1 SM slot and 1 NIM slot, and 6 x 1-Gigabit Ethernet ports)**			
	SD-WAN IPsec Throughput (1400Bytes	**1.9Gbps**			
	SD-WAN IPsec Throughput (IMIX*)	**1.75Gbps**			
	Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), Internet Key Exchange (IKE), Access Control Lists (ACL), Configuration Protocol (DHCP), (HSRP), RADIUS			
	SD-WAN Overlay Tunnels scale	**6000**			
	IPv4 Forwarding Throughput (1400Bytes)	**19.7Gbps**			
	IPsec Throughput (1400Bytes)	**1.9Gbps**			
	Number of IPsec SVTI Tunnels	**4000**			
	Number of ACLs per system	**4000**			
	Number of IPv4 ACEs per system	**72K**			
	Number of IPv4 Routes	**1.6M w/ default 8GB, up to 4M w/ 32GB**			
	Number of	**1.5M w/ default 8GB, up to 4M w/**			

	IPv6 Routes	**32GB**			
	Number of Queues	**16K**			
	Number of NAT Sessions	**1.2M w/ default 8GB, up to 2M w/ 32GB**			
	Number of Firewall Sessions	**512K**			
	Number of VRFs	**4000**			
	Power maximum rating	**400 W**			
	Cryptographic algorithms	**Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes) Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit) Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512**			
	Dual power supplies	**Yes**			
Lotul 2. Echipamentul firewall de generație următoare (NGFW)					
1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). 8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a	**5 bucăți**	**180 000,00**	**1800,00**

traficului pe un singur pas. 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1. **Aplicații corporative:** 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin;			

17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; **17.2. Aplicații Internet**: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv ICQ, Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video, inclusiv Skype; 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodoare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu,			

	controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: • Permisiune sau interdicție; • Permisiunea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni; • Permisiune, dar cu scanare pentru viruși și alte amenințări; • Permisiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirecționării traficului pe bază de politici			

(Policy Based Forwarding); • Permisiunea anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2003, 2007 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă			

există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare):Duo, • Okta, • RSA SecureID,			

• PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 67. **Cerințe pentru sistemul de management centralizat:** • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi			

exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Platforma trebuie să suporte gestionarea a cel puțin 1000 de echipamente firewall de nouă generație (NGFW); • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport			

LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. **Managementul rolurilor administratorilor locali:** • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele **HTTPS** și **SSH**, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. **Cerințe de performanță ale firewall-ului:** **Performance:** • Threat prevention throughput 0.8 Gbps; • IPsec VPN throughput 650 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; • Max sessions (IPv4 or IPv6) 64,000. **Policies:** • Security rules 500; • Security rule schedules 256; • NAT rules 400; • Decryption rules 100; • App override rules 100; • Tunnel content inspection rules 100; • SD-WAN rules 100; • Policy based forwarding rules 100; • Captive portal rules 10; • DoS protection rules 100. **Security Zones:** • Max security zones 25.			

Objects (addresses and services): • Address objects 2500; • Address groups 125; • Members per address group 2,500; • Service objects 1,000; • Service groups 250; • Members per service group 500; • FQDN address objects 2,000; • Max DAG IP addresses 1000; • Tags per IP address 32. **Security Profiles:** • Security profiles 75. **SSL Decryption:** • Max SSL inbound certificates 25; • Max concurrent decryption sessions 6600; **URL Filtering:** • Total entries for allow list, block list and custom categories 25,000; • Max custom categories 2,849; • Max custom categories (virtual system specific) 500; **Interfaces:** • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2). **Storage Capacity:** • 64 GB eMMC **Virtual Routers:** • Virtual routers 3. **Routing:** • IPv4 forwarding table size 5,000; • IPv6 forwarding table size 2500; • System total forwarding table size 5,000; • Max routing peers (protocol dependent) 500; • Static entries - DNS proxy 1,024. **L2 Forwarding:** • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; • Max ARP entries per broadcast domain 1500; • Max MAC entries per broadcast domain 1500. **NAT:** • Total NAT rule capacity 400; • Max NAT rules (static) 400; • Max NAT rules (DIP) 400; • Max NAT rules (DIPP) 200; • Max translated IPs (DIP) 16000; • Max translated IPs (DIPP) 200. **Address Assignment:** • DHCP servers 3; • DHCP relays 500; • Max number of assigned addresses 64,000.			

High Availability: • Devices supported 2; • Max virtual addresses 32. **QoS:** • Number of QoS policies 1,000; • Physical interfaces supporting QoS 8; • Clear text nodes per physical interface 31. **IPSec VPN:** • Max IKE Peers 1000; • Site to site (with proxy id) 1000; • SD-WAN IPsec tunnels 1000.			
Termen de garanție 12 luni			

Condiții specifice de eligibilitate și executare a contractului:

1. **Garanție și suport tehnic:**
   - Furnizorul va asigura o garanție completă pentru hardware și software (HW+SW) pe o perioadă de 12 luni de la data recepției finale a echipamentelor.
   - În perioada de garanție, producătorul echipamentului va furniza suport tehnic la distanță (prin e-mail sau conectare remote), iar partenerul local al producătorului va asigura asistență tehnică la fața locului, la solicitarea autorității contractante.
2. **Servicii incluse în ofertă:**
   - Ofertantul este responsabil de:
     - livrarea,
     - instalarea,
     - configurarea,
     - punerea în funcțiune a echipamentelor,
     - instruirea personalului desemnat de autoritatea contractantă (training).
   - Toate aceste servicii vor fi incluse în prețul total al ofertei comerciale, fără costuri suplimentare.
3. **Calificarea personalului tehnic:**
   - Ofertantul va prezenta certificate valabile care atestă că minimum doi specialiști proprii (nu delegați prin parteneriate) dețin competențe tehnice avansate pentru echipamentul ofertat.
4. **Autorizare oficială din partea producătorului:**
   - Este obligatorie prezentarea Autorizării oficiale (MAF) emise de producător, care confirmă că ofertantul este reprezentant autorizat pentru livrarea, instalarea și întreținerea echipamentelor pe teritoriul Republicii Moldova.
   - Autorizarea trebuie să fie valabilă pentru procedura de achiziție în cauză și prezentată în original sau copie legalizată.
5. **Certificare în domeniul securității informaționale:**
   - Ofertantul trebuie să dispună de cel puțin o persoană certificată în calitate de auditor intern pentru sistemul de management al securității informaționale, în conformitate cu standardul ISO 27001:2013.
6. **Experiență relevantă:**
   - Ofertantul va demonstra experiență anterioară prin prezentarea a cel puțin 3 contracte de livrare și instalare a echipamentelor de tip NGFW (Next Generation Firewall) executate cu succes în ultimii 3 ani.
7. **Termen de livrare:**
   - Echipamentele vor fi livrate și puse în funcțiune în termen de maximum 90 de zile calendaristice de la data intrării în vigoare a contractului.

9. În cazul procedurilor de preselecție se indică numărul minim al candidaților 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 (se va selecta):

1). Pentru fiecare lot în parte

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

12. Termenii și condițiile de livrare/prestare/executare solicitați: *Timp de 90 zile din data înaintării comunicării către Vînzător privind transmiterea dării de seama la Agenţia Achiziţii Publice, cu livrare și descărcare a bunurilor la depozitul CNAS din str. Gheorghe Tudor nr. 3 mun. Chișinău***.**

13. Termenul de valabilitate a contractului : *31.12.2025*

***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; 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	Prezentarea Cererii de participare conform ***Anexei nr.7*** din Ordinul MF 115/2021**.**	Cerere de participare confirmată prin semnătura electronică	***Obligatoriu***
2	Prezentarea Declaraţiei privind valabilitatea ofertei conform ***Anexei nr.8*** din Ordinul MF 115/2021	Declaraţia privind valabilitatea ofertei confirmată prin semnătura electronică	***Obligatoriu***
3	Prezentarea Specificații 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 şi-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.	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***
7	Vor fi excluși operatorii economici care nu dispun de standarde de asigurare a calităţii	**Declarație pe propria răspundere privind.** **1. Garanție și suport tehnic:** o Furnizorul va asigura o garanție completă pentru hardware și software (HW+SW) pe o perioadă de 12 luni de la data recepției finale a echipamentelor. o În perioada de garanție, producătorul echipamentului va furniza suport tehnic la distanță (prin e-mail sau conectare remote), iar partenerul local al producătorului va asigura asistență tehnică la fața locului, la solicitarea autorității contractante. **2. Servicii incluse în ofertă:** o Ofertantul este responsabil de: ▪ livrarea, ▪ instalarea, ▪ configurarea, ▪ punerea în funcțiune a echipamentelor, ▪ instruirea personalului desemnat de autoritatea contractantă (training). o Toate aceste servicii vor fi incluse în prețul total al ofertei comerciale, fără costuri suplimentare. **3. Autorizare oficială din partea producătorului:** o Este obligatorie prezentarea Autorizării oficiale (MAF) emise de producător, care confirmă că ofertantul este reprezentant autorizat pentru livrarea, instalarea și întreținerea echipamentelor pe teritoriul Republicii Moldova. o Autorizarea trebuie să fie valabilă pentru procedura de achiziție în cauză și prezentată în original sau copie legalizată.	***Obligatoriu***
9	Vor fi excluși operatorii economici care nu dispun de capacitatea tehnică şi profesională	**Declarație pe propria răspundere privind.** **1. Calificarea personalului tehnic:** o Ofertantul va prezenta certificate valabile care atestă că minimum doi specialiști proprii (nu delegați prin parteneriate)	***Obligatoriu***

		deţin competenţe tehnice avansate pentru echipamentul ofertat. **2. Certificare în domeniul securității informaționale:** o Ofertantul trebuie să dispună de cel puțin o persoană certificată în calitate de auditor intern pentru sistemul de management al securității informaționale, în conformitate cu standardul ISO 27001:2013. **3. Experiență relevantă:** Ofertantul va demonstra experiență anterioară prin prezentarea a cel puțin 3 contracte de livrare și instalare a echipamentelor de tip NGFW (Next Generation Firewall) executate cu succes în ultimii 3 ani.	
10	Va fi exclus orice operator economic care nu deţine numărul de înregistrare a producătorului în Lista producătorilor	Declarație pe propria răspundere privind numărul de înregistrare a producătorului de echipamente electrice și electronice în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor (HG 212/2018) - confirmată prin semnătura electronică a Participantului	***Obligatoriu***
11	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*** *Lipsa condamnări i pe parcursul a ultimilor 5 ani.*
12	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 insolvabilitat e*
13	DECLARAŢIE privind confirmarea identității beneficiarilor efectivi și	Declarație în conformitate cu **Anexa nr. 2** autentificată prin aplicarea semnăturii electronice a Participantului – depunere	***Da*** – *depunere obligatorie*

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

Anexa nr. 2

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

DECLARAŢIE
privind confirmarea identității beneficiarilor efectivi și 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 și/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): licitația electronică, 3 runde , pasul minim pentru fiecare lot în parte Lot 1 – 1 500,00 lei,Lot 2 – 1 800,00
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.	Denumirea factorului de evaluare	Ponderea%

d/o		
	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 M-Tender.*
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 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: *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. 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: _____

Președinta grupului de lucru: _____ **Maia Moraru**
L.Ș.

Anexa nr. 7
la Documentația standard nr._____
din "____" _____ 20___

CERERE DE PARTICIPARE

Către_____
(denumirea autorităţii contractante şi adresa completă)

Stimaţi domni,

Ca urmare a anunțului/invitației de participare/de preselecție apărut în Buletinul achizițiilor publice și/sau Jurnalul Oficial al Uniunii Europene, nr. . . . . din . . . . . (ziua/luna/anul), privind aplicarea procedurii pentru atribuirea contractului . . . . . (denumirea contractului de achiziție publică), noi . . . . . (denumirea/numele ofertantului/candidatului), am luat cunoștință de condițiile și de cerințele expuse în documentația de atribuire și exprimăm prin prezenta interesul de a participa, în calitate de ofertant/candidat, neavînd obiecții la documentația de atribuire.

Data completării . . . . . Cu stimă,

Ofertant/candidat

. . . . . .

(semnătura autorizată)

Anexa nr. 8
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE
privind valabilitatea ofertei

Către_____
(*denumirea autorităţii contractante şi adresa completă*)

Stimaţi domni,

Ne angajăm să menținem oferta valabilă, **privind achiziționarea _____**
(se indică obiectul achiziției)
prin procedura de achiziție_____,
(tipul procedurii de achiziție)
pentru o durată de _____ zile, (durata în litere și cifre), respectiv până la data de _____ (ziua/luna/anul), și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării . . . . . Cu stimă,

Ofertant/candidat

. . . . . .

(semnătura autorizată)

Anexa nr. 9
la Documentația standard nr._____
din "____" _____ 20___

BANCA

_____
(denumirea)

SCRISOARE DE GARANŢIE BANCARĂ

pentru participare cu ofertă la procedura de atribuire a contractului de achiziţie publică

Către_____
(denumirea autorităţii contractante şi adresa completă)
_____
cu privire la procedura de atribuire a contractului
_____,
(denumirea contractului de achiziţie publică)
subsemnaţii_____,
(denumirea băncii)
Înregistrat la_____,
(adresa băncii)
ne obligăm faţă de _____să
(*denumirea autorităţii contractante*)
plătim suma de_____, la prima sa cerere scrisă şi
(suma în litere şi în cifre)

fără ca acesta să aibă obligaţia de a-şi motiva cererea respectivă, cu condiţia, ca în cererea sa autoritatea contractantă să specifice că suma cerută de ea şi datorată ei este din cauza existenţei uneia sau mai multora dintre situaţiile următoare:

1. Ofertantul _____
(denumirea ofertantului)
îşi retrage sau modifică oferta în perioada de valabilitate a acesteia;
Prezenta ofertă rămâne valabilă pentru perioada de timp specificată în Anexa nr.2 Anunțul de Participare, începînd cu data-limită pentru depunerea ofertei, în conformitate cu Anexa nr.2 Anunțul de Participare, și rămâne obligatorie şi poate fi acceptată în orice moment până la expirarea acestei perioade;
2. Oferta sa fiind stabilită câştigătoare, ofertantul _____
(denumirea ofertantului)
nu a constituit garanţia de bună execuție;
3. Oferta sa fiind stabilită câştigătoare, ofertantul _____
(denumirea ofertantului)
a refuzat să semneze contractul de achiziţie publică de bunuri/servicii;

Nu se execută vreo condiţie, specificată în documenația de atribuire înainte de semnarea contractului de achiziţie publică de bunuri/servicii.
Prezenta garanţie este valabilă până la data de _____
Parafată de Banca_____în ziua___luna____anul_____
(semnătura autorizată)

Anexa nr. 10
la Documentația standard nr._____
din "____" _____ 20___

[Banca comercială, la cererea ofertantului cîştigător, va completa acest formular pe foaie cu antet, în conformitate cu instrucţiunile de mai jos.]

Data: "___" _____ 20__

Procedura de achiziție Nr.: _____

Oficiul Băncii: _____
[introduceţi numele complet al garantului]

Beneficiar: _____
[introduceţi numele complet al autorităţii contractante]

GARANŢIA DE BUNĂ EXECUŢIE
Nr. _____

Noi, *[introduceţi numele legal şi adresa băncii],* am fost informaţi că firmei *[introduceţi numele deplin al Furnizorului/Prestatorului]* (numit în continuare „Furnizor/Prestator") i-a fost adjudecat Contractul de achiziție publică de livrare/prestare _____ [*obiectul achiziţiei, descrieţi bunurile/serviciile*] conform anunțului/invitaţiei la procedura de achiziție nr. din _____. 20_ [*numărul şi data procedurii de achiziție*] (numit în continuare „Contract").

Prin urmare, noi înţelegem că Furnizorul/Prestatorul trebuie să depună o Garanţie de bună execuţie în conformitate cu prevederile documentației de atribuire.

În urma solicitării Furnizorul/Prestatorului, noi, prin prezenta, ne angajăm irevocabil să vă plătim orice sumă(e) ce nu depăşeşte *[introduceţi suma(ele) în cifre şi cuvinte]* la primirea primei cereri în scris din partea Dvs., prin care declaraţi că Furnizorul/Prestatorul nu îndeplineşte una sau mai multe obligaţii conform Contractului, fără discuţii sau clarificări şi fără necesitatea de a demonstra sau arăta temeiurile sau motivele pentru cererea Dvs. Sau pentru suma indicată în aceasta.

Această Garanţie va expira nu mai tîrziu de *[introduceţi numărul]* de la data de *[introduceţi luna][introduceţi anul]*, şi orice cerere de plată ce ţine de aceasta trebuie recepţionată de către noi la oficiu pînă la această dată inclusiv.

[semnăturile reprezentanţilor autorizaţi ai băncii şi ai Furnizorului/Prestatorului]

Anexa nr. 11
la Documentația standard nr._____
din "____" _____ 20___

INFORMAŢII PRIVIND ASOCIEREA

1.Părţi contractante (agenţi economici)

a) _____
b) _____
c) _____

2. Adrese, telefon, fax a oficiilor partenerilor (părţi contractante):

a) _____
b) _____
c) _____

3. Informaţii privind modul de asociere:

a) Data încheierii contractului de asociere _____

b) Locul şi data înregistrării asociaţiei_____

c)Activităţi economice ce se vor realiza în comun _____

d) Contribuţia fiecărei părţi la realizarea activităţilor economice comune convenite _____

_____

e) Valoarea și cota procentuală a bunurilor livrate/serviciilor prestate de fiecare asociat

f) Condiţii de administrare a asociaţiei_____

g)Modalitatea de împărţire a rezultatelor activităţii economice comune desfăşurate _____

h)Cauze de încetare a asociaţiei şi modul de împărţire a rezultatelor lichidării_____

i) Repartizarea fizică, valorică şi procentuală între fiecare asociat pentru executarea obiectivului supus licitaţiei_____

j) Alte cauze_____

Data completării _____
Semnat Liderul Asociației: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Semnat Asociatul secund: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr. 12
la Documentația standard nr._____
din "____" _____ 20___

DECLARAȚIE
privind lista principalelor livrari/prestări efectuate în ultimii 3 ani de activitate

Nr d/o	Obiectul contractului	Denumirea/ numele beneficiarului/Adresa	Calitatea Furnizorului/Prestatorului*)	Preţul contractului/ valoarea bunurilor/serviciilor livrate/prestate	Perioada de livrare/prestare (luni)
1					
2					
...					

*) Se precizează calitatea în care a participat la îndeplinirea contractului, care poate fi de: contractant unic sau lider de asociaţie; contractant asociat; subcontractant.

Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr. 13
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE
privind dotările specifice, utilajul şi echipamentul necesar pentru îndeplinirea corespunzătoare a contractului

Nr. d/o	Denumirea principalelor utilaje, echipamente, mijloace de transport, baze de producţie (ateliere, depozite, spaţii de cazare) şi laboratoare propuse de ofertant ca necesare pentru prestarea serviciilor, rezultate în baza tehnologiilor pe care el urmează să le adopte	Unitatea de măsură (bucăţi şi seturi)	Asigurate din dotare	Asigurate de la terţi sau din alte surse
0	**1**	**2**	**3**	**4**
1.				
2.				
3.				
.				
n				

Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____

Denumirea firmei: _____

Anexa nr.15
la Documentația standard nr._____
din "____" _____ 20___

LISTA SUBCONTRACTANȚILOR
ŞI PARTEA/PĂRȚILE DIN CONTRACT CARE SUNT
ÎNDEPLINITE DE ACEŞTIA

Nr. d/o	**Numele şi adresa subantreprenorilor**	**Activităţi din contract**	**Valoarea aproximativă**	**% din valoarea contractului**
1.				
2.				
3.				
4.				

Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr.16
la Documentația standard nr._____
din "____" _____ 20___

ANGAJAMENT TERŢ SUSŢINĂTOR FINANCIAR

Terţ susţinător financiar

.....(denumirea)

ANGAJAMENT
privind susţinerea financiară a ofertantului/candidatului

Către, ...

(denumirea autorităţii contractante şi adresa completă)
Cu privire la procedura pentru atribuirea contractului .....
(denumirea contractului de achiziţie publică), noi .....(*denumirea terţului susţinător financiar)*, având sediul înregistrat la ..... (*adresa terţului susţinător financiar)*, ne obligăm, în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia ..... (*denumirea ofertantului/candidatului*) toate resursele financiare necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor asumate de acesta conform ofertei prezentate şi contractului de achiziţie publică ce urmează a fi încheiat între ofertant şi autoritatea contractantă.
Acordarea susţinerii financiare nu implică alte costuri pentru achizitor, cu excepţia celor care au fost incluse în propunerea financiară.
În acest sens, ne obligăm în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia .....(*denumirea ofertantului/candidatului)* suma de .....(valoarea totală/parţială din propunerea financiară), necesară pentru îndeplinirea integrală, reglementară şi la termen a contractului de achiziţie publică.
Noi, ... (*denumirea terţului susţinător financiar),* declarăm că înţelegem să răspundem faţă de autoritatea contractantă pentru neexecutarea oricărei obligaţii asumate de ..... (*denumirea ofertantului)*, în baza contractului de achiziţie publică şi pentru care ..... (*denumirea ofertantului/candidatului)* a primit susţinerea financiară conform prezentului angajament, renunţând în acest sens, definitiv şi irevocabil, la invocarea beneficiului de diviziune.
Noi, ... *(denumirea terţului susţinător financiar)*, declarăm că înţelegem să renunţam definitiv şi irevocabil la dreptul de a invoca orice excepţie de neexecutare, atât faţă de autoritatea contractantă, cât şi faţă de ..... (*denumirea ofertantului/candidatului),* care ar putea conduce la neexecutarea, parţială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligaţiilor asumate de noi prin prezentul angajament.
Noi,..... *(denumirea terţului susţinător financiar),* declarăm că înţelegem să răspundem pentru prejudiciile cauzate autorităţii contractante ca urmare a nerespectării obligaţiilor prevăzute în angajament.
Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.21 alin.(6) al Legii nr.131/2015 privind achiziţiile publice, care dă dreptul autorităţii contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligaţii care decurg din susţinerea financiară acordată ..... (*denumirea ofertantului/candidatului).*

Data completării,
.....

Terţ susţinător,
.....
(semnătură autorizată)

Anexa nr. 17
la Documentaţia standard nr._____
din "____" _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR FINANCIAR

Terţ susţinător financiar

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al ..... (*denumirea terţului susţinător financiar),* declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că toate

resursele financiare necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor contractului de achiziţie publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiţionat, în funcţie de necesităţile care vor apărea pe parcursul îndeplinirii contractului de achiziţie publică având ca obiect.....(*obiectul contractului).*

Data completării, Terţ susţinător,

(*semnătură autorizată*)

Anexa nr. 18
la Documentaţia standard nr._____
din "____" _____ 20___

ANGAJAMENT PRIVIND SUSŢINEREA TEHNICĂ ŞI PROFESIONALĂ A OFERTANTULUI/GRUPULUI DE OPERATORI ECONOMICI

.....
(denumirea)

ANGAJAMENT
privind susţinerea tehnică şi profesională
a ofertantului/candidatului

Către, ...
(denumirea autorităţii contractante şi adresa completă)
Cu privire la procedura pentru atribuirea contractului ..... *(denumirea contractului de achiziţie publică),* noi ..... *(denumirea terţului susţinător tehnic şi profesional*), având sediul înregistrat la ....*(adresa terţului susţinător tehnic şi profesional)*, ne obligăm, în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia..... (*denumirea ofertantului)* toate resursele tehnice şi profesionale necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor asumate de acesta, conform ofertei prezentate şi contractului de achiziţie publică ce urmează a fi încheiat între ofertant şi autoritatea contractantă.
Acordarea susţinerii tehnice şi profesionale nu implică alte costuri pentru achizitor, cu excepţia celor care au fost incluse în propunerea financiară.
În acest sens, ne obligăm în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia ..... (*denumirea ofertantului/candidatului)* resursele tehnice şi/sau profesionale de ....necesare pentru îndeplinirea integrală, reglementară şi la termen a contractului de achiziţie publică.
Noi, ... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să răspundem, în mod necondiţionat, faţă de autoritatea contractantă pentru neexecutarea oricărei obligaţii asumate de ..... *(denumire ofertantului/candidatului)*, în baza contractului de achiziţie publică, şi pentru care ..... *(denumirea operatorului/candidatului)* a primit susţinerea tehnică şi profesională conform prezentului angajament, renunţând în acest sens, definitiv şi irevocabil, la invocarea beneficiului de diviziune.
Noi, ... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să renunţăm definitiv şi irevocabil la dreptul de a invoca orice excepţie de neexecutare, atât faţă de

autoritatea contractantă, cât şi faţă de ..... (*denumire ofertant),* care ar putea conduce la neexecutarea, parţială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligaţiilor asumate de noi prin prezentul angajament.
Noi,..... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să răspundem pentru prejudiciile cauzate autorităţii contractante ca urmare a nerespectării obligaţiilor prevăzute în angajament.
Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.22 alin.(6) al Legii nr.131/2015 privind achizițiile publice, care dă dreptul autorităţii contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligaţii care decurg din susţinerea tehnică şi profesională acordată ..... (*denumirea ofertantului/candidatului).*

Data completării,
.....

Terţ susţinător,
.....
(semnătură autorizată)

Anexa nr. 19
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR TEHNIC

Terţ susţinător tehnic

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al ..... (*denumirea terţului susţinător tehnic),* declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind logistica, utilajele, instalaţiile, echipamentele tehnice de care dispun şi care urmează a fi folosite efectiv pentru îndeplinirea contractului de achiziţie publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiţionat, în funcţie de necesităţile care vor apărea pe parcursul îndeplinirii contractului de achiziţie publică având ca obiect.....(*obiectul contractului).*

LISTA

privind logistica, utilajele, instalaţiile şi echipamentele tehnice aflate în dotare și care urmează a fi efectiv folosite pentru îndeplinirea contractului de achiziţie publică

Nr.	Denumire	Cantitate	Forma de deţinere

crt	utilaj/echipament/instalaţie	U.M.		
			Proprietate	În chirie

Prezenta declaraţie este anexă la „Angajamentul ferm” privind susţinerea noastră tehnică şi profesională oferită.....(*denumirea ofertantului/candidatului).*

Data completării, Terţ susţinător,

(semnătură autorizată)

Anexa nr. 20
la Documentaţia standard nr._____
din “____” _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR PROFESIONAL

Terţ susţinător profesional

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al .....(denumirea terţului susţinător profesional), declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind efectivul mediu anual al personalului de specialitate angajat care urmează a fi efectiv alocat pentru îndeplinirea contractului de achiziţie publică..... sunt reale.

LISTA

privind personalul de specialitate angajat care urmează a fi efectiv alocat pentru îndeplinirea contractului de achiziţie publică

	Anul 1	Anul 2	Anul 3
Personalul de specialitate			
……			
……			
…….			

Anexez declaraţiei, CV-urile personalului de specialitate, precum şi ale personalului care va fi alocat efectiv pentru îndeplinirea contractului de achiziţie publică.

Subsemnatul declar că informaţiile furnizate, referitoare la experienţa anterioară, capacităţile tehnice şi personalul de specialitate angajat sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, situaţiilor şi documentelor care însoţesc oferta, orice informaţii suplimentare în scopul verificării datelor din prezenta declaraţie.

Subsemnatul autorizez prin prezenta orice instituţie, societate comercială, bancă, alte persoane juridice să furnizeze informaţii reprezentanţilor autorizaţi ai ..... (*denumirea şi adresa autorităţii contractante)* cu privire la orice aspect tehnic şi financiar în legătură cu activitatea noastră.

Prezenta declaraţie este anexă la „Angajamentul ferm" privind susţinerea noastră tehnică şi profesională oferită ....(*denumirea ofertantului/candidatului).*

Data completării, Terţ susţinător,

(semnătură autorizată)

Anexa nr. 21
la Documentația standard nr._____
din "____" _____ 20___

CAIET DE SARCINI
Bunuri/Servicii

Obiectul_____
(denumirea, adresa)
Autoritatea contractantă_____
(denumirea, adresa)

1. Descriere generală. Informaţii

Se dau detalii generale privind obiectul achiziției.

2. Utilizarea, păstrarea, protecţia, calitatea produselor/serviciilor

Se precizează detalii privind modul de transportare, prestare, utilizare și locul livrării/prestării a produselor/serviciilor.

3. Materiale, compatibilităţi, reglementări tehnice şi standarde utilizate

Se precizează conformitatea şi aplicabilitatea materialelor, legislaţia, reglementările tehnice şi standardele aplicate.

4. Cerinţe privind calculul costului/prețului

Se precizează modalitatea de calculare a costului bunului/serviciului, prin trimitere la actele normative în domeniu.

5. Mostre

Se precizează modul de prezentare a mostrelor la toate produsele utilizate.

6. Echipamentele, instalaţiile, utilajele, sculele, instrumentele, dispozitivele şi alte obiecte necesare pentru prestarea serviciilor

Se precizează echipamentele, instalaţiile, utilajele, sculele, instrumentele, dispozitivele, mijloacele de transport, etc..

7. Articole, produse şi piese necesare instalaţiilor

Se precizează furnizorul articolelor, produselor şi pieselor necesare instalaţiilor, tipurile şi cantitatea.

8. Definiţii

Se precizează termenii şi definiţiile utilizate în caietul de sarcini şi unele caracteristici.

9. Documente obligatorii la depunerea ofertei

La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate la depunerea ofertei prin intermediul SIA RSAP. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți.

10. Documente obligatorii la evaluarea ofertelor

La punctul dat autoritatea contractantă indică care documente sunt obligatorii de a fi prezentate în SIA RSAP la evaluarea ofertei. La fel, tot aici se indică documentele ce conțin date cu caracter personal, care nu se depun prin intermediul SIA RSAP și nu sunt publice pentru toți, ele se prezintă la etapa de evaluare direct autorității contractante.

Autoritatea contractantă _____ Data „____”_____

Notă: *Prezentul model al caietului de sarcini este orientativ şi poate fi completat, modificat, precizat de către autoritatea contractantă, în funcţie de tipul şi specificul bunurilor/serviciilor. Autoritatea contactantă este obligată să respecte legislația.*

Anexa nr. 2
la Caietul de sarcini

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

DECLARAŢIE
privind confirmarea identității beneficiarilor efectivi și 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 _____

Anexa nr.22
la Documentația standard nr._____
din "____" _____ 20___

Specificaţii tehnice

[AAcest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție_____din_____
Obiectul achiziției:_____

Denumirea bunurilor	**Denumirea modelului bunului**	**Ţara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**		**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5		6	7
Lotul 1 ***Anexa nr. 1***							
Lotul 1. ***Router***				Type	Router **CISCO C8300-1N1S-6T care va permite funcționarea în regim standby**		**Moldova Standard**
				Rack Units (RU)	1RU		
				Memory (DRAM) default	8 GB		
				Storage (M.2 SSD)	16 GB		
				Flash memory support	8 G		
				Interface	1x1G WAN (1 SM slot and 1 NIM slot, and 6 x 1-Gigabit Ethernet ports)		

					SD-WAN IPsec Throughput (1400Bytes	1.9Gbps		
					SD-WAN IPsec Throughput (IMIX*)	1.75Gbps		
					Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), Internet Key Exchange (IKE), Access Control Lists (ACL), Configuration Protocol (DHCP), (HSRP), RADIUS			
					SD-WAN Overlay Tunnels scale	6000		
					IPv4 Forwarding Throughput (1400Bytes)	19.7Gbps		
					IPsec Throughput (1400Bytes)	1.9Gbps		
					Number of IPsec SVTI Tunnels	4000		
					Number of ACLs per system	4000		
					Number of IPv4 ACEs per system	72K		

				Number of IPv4 Routes	1.6M w/ default 8GB, up to 4M w/ 32GB		
				Number of IPv6 Routes	1.5M w/ default 8GB, up to 4M w/ 32GB		
				Number of Queues	16K		
				Number of NAT Sessions	1.2M w/ default 8GB, up to 2M w/ 32GB		
				Number of Firewall Sessions	512K		
				Number of VRFs	4000		
				Power maximum rating	400 W		
				Cryptographic algorithms	Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes) Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit) Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512		
				Dual power supplies	Yes		
Lotul 2. Echipamentul firewall de generație următoare (NGFW)				1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). 8. Firewall-ul NGFW propus			

				trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate. 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: 17.1 . Aplicații corporative: 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. 17.1.4. ERP, CRM, inclusiv SAP, 1C; 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii		

				utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv ICQ, Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video, inclusiv Skype; 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodoare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor		

				care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: • Permisiune sau interdicție; • Permisiunea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni; • Permisiune, dar cu scanare pentru viruși și alte amenințări; • Permisiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe		

				aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirecționării traficului pe bază de politici (Policy Based Forwarding); • Permisiunea anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare		

				necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2003, 2007 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie		

				să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare):Duo, • Okta, • RSA SecureID, • PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor.		

				67. Cerințe pentru sistemul de management centralizat: • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Platforma trebuie să suporte gestionarea a cel puțin 1000 de echipamente firewall de nouă generație (NGFW); • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe.		

				70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 0.8 Gbps; • IPsec VPN throughput 650 Mbps;		

				• Connections per second 1100; • Firewall throughput 1.4 Gbps; • Max sessions (IPv4 or IPv6) 64,000. Policies: • Security rules 500; • Security rule schedules 256; • NAT rules 400; • Decryption rules 100; • App override rules 100; • Tunnel content inspection rules 100; • SD-WAN rules 100; • Policy based forwarding rules 100; • Captive portal rules 10; • DoS protection rules 100. Security Zones: • Max security zones 25. Objects (addresses and services): • Address objects 2500; • Address groups 125; • Members per address group 2,500; • Service objects 1,000; • Service groups 250; • Members per service group 500; • FQDN address objects 2,000; • Max DAG IP addresses 1000; • Tags per IP address 32. Security Profiles: • Security profiles 75. SSL Decryption: • Max SSL inbound certificates 25; • Max concurrent decryption sessions 6600; URL Filtering: • Total entries for allow list, block list and custom categories 25,000; • Max custom categories 2,849; • Max custom categories (virtual system specific) 500; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2). Storage Capacity: • 64 GB eMMC Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size 5,000; • IPv6 forwarding table size 2500; • System total forwarding table size 5,000; • Max routing peers (protocol dependent) 500; • Static entries - DNS proxy 1,024. L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; • Max ARP entries per broadcast domain 1500; • Max MAC entries per broadcast domain 1500. NAT: • Total NAT rule capacity 400; • Max NAT rules (static) 400; • Max NAT rules (DIP) 400;		

				• Max NAT rules (DIPP) 200; • Max translated IPs (DIP) 16000; • Max translated IPs (DIPP) 200. Address Assignment: • DHCP servers 3; • DHCP relays 500; • Max number of assigned addresses 64,000. High Availability: • Devices supported 2; • Max virtual addresses 32. QoS: • Number of QoS policies 1,000; • Physical interfaces supporting QoS 8; • Clear text nodes per physical interface 31. IPSec VPN: • Max IKE Peers 1000; • Site to site (with proxy id) 1000; • SD-WAN IPsec tunnels 1000		

Semnat:_____ Numele, Prenumele:_____ În calitate de: _____

Ofertantul: _____ Adresa: _____

Anexa nr.23
la Documentația standard nr._____
din "____" _____ 20___

Specificații de preț

[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8 și 11 la necesitate, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]

Numărul procedurii de achiziție_____din_____

Obiectul de achiziției:_____

Cod CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare/prestare	Clasificație bugetară (IBAN)	Discount %
1	2	3	4	5	6	7	8	9	10	11
Lotul nr. 1										
32420000-3	***Lotul 1. Router CISCO C8300-1N1S-6T care va permite funcționarea în regim standby***	buc	1					*Timp de 90 zile din data întrării în vigoare a contractului cu livrare și descărcare a în*	MD84TRPFAH518710A01691AA	

								depozitul CNAS din str. Gheorghe Tudor nr. 3.		
Lotul nr. 2										
32420000-3	***Lotul 2 . Echipamentul firewall de generație următoare (NGFW)***	buc	5					*Timp de 90 zile din data întrării în vigoare a contractului cu livrare și descărcare a în depozitul CNAS din str. Gheorghe Tudor nr. 3.*	MD84TRPFAH518710A01691AA	

Semnat:_____ Numele, Prenumele:_____ În calitate de: _____

Ofertantul: _____ Adresa: _____

Anexa nr. 24
la Documentația standard nr._____
din "____" _____ 20___

A C H I Z I Ţ I I P U B L I C E

CONTRACT Nr.
privind achiziţia de bunuri

I PARTEA GENERALĂ

Obiectul achiziției: ***Echipament pentru asigurarea funcționării rețelei corporative***

Cod CPV: ***32420000-3***

"___"_____20__ *mun. Chișinău*

Vînzător	Cumpărător
_____, *(denumirea completă a întreprinderii, asociaţiei, organizaţiei)* reprezentată prin _____, *(funcţia, numele, prenumele)* care acţionează în baza _____, *(statut, regulament, hotărîre etc.)* denumit(a) în continuare *Vînzător*, _____, *(se indică nr. şi data de înregistrare în Registrul de Stat)* pe de o parte,	**Casa Naţională de Asigurări Sociale,** reprezentată prin Directoare generală Dna ŢÎBÎRNĂ Elena, care acţionează în baza regulamentului cu privire la organizarea și funcționarea Casei Naţionale de Asigurări Sociale (HG. 230/2020), înregistrat la camera înregistrării de stat IDNO 1004600030235 denumit(a) în continuare *Beneficiar*, pe de altă parte,

ambii (denumiţi(te) în continuare Părţi), au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea ***Echipamentului pentru asigurarea funcționării rețelei corporative***
,
(denumirea bunului/serviciului)
denumite în continuare Bunuri, conform procedurii de achiziţii publice de tip _____ nr._____ din_____,
în baza deciziei grupului de lucru al Cumpărătorului din „___” _____20__.

b. Următoarele documente vor fi considerate părţi componente ale Contractului:
a) Specificaţia tehnică..... ***Anexa nr.1***;
b) Specificația de preț..... ***Anexa nr.2***;
c) Act de instalare …….***Anexa nr. 3;(pentru Lotul 1)***

c. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.
d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, se obligă prin prezentul contract să livreze Cumpărătorului Bunurile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.
e. Cumpărătorul se obligă prin prezentul contract să plătească Vînzătorului, în calitate de contravaloare a livrării bunurilor, prețul Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1. Vînzătorul îşi asumă obligaţia de a livra Bunurile conform Specificaţiei tehnice din ***Anexa nr.1*** și Specificația de preț din ***Anexa nr.2*** care este parte integrantă a prezentului Contract.
1.2. Cumpărătorul se obligă, la rîndul său, să achite şi să recepţioneze Bunurile livrate de Vînzător.
1.3. Termenele de garanţie a bunurilor livrate este 12 luni.

2. Termeni şi condiţii de livrare

2.1. Livrarea Bunurilor se efectuează de către Vînzător *Timp de 120 zile din data înaintării comunicării către Prestator privind transmiterea dării de seamă la Agenţia Achiziţii Publice, şi cu livrare și descărcare a bunurilor: în depozitul CNAS din str. Gheorghe Tudor nr. 3*.
2.2. Documentaţia de însoţire a Bunurilor include:
1) *Originalele facturilor fiscale* ……..... 2 ex
2) Act de instalare ***Anexa nr. 3; (pentru Lotul 1)*** ……. 2 ex

2.3. Originalele documentelor prevăzute în punctul 2.2 se vor prezenta Cumpărătorului cel tîrziu la momentul livrării bunurilor la destinaţia finală. Livrarea bunurilor se consideră încheiată în momentul în care sînt prezentate documentele de mai sus.

3. Preţul şi condiţii de plată

3.1.Preţul Bunurilor livrate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat Specificaţia prezentului Contract.

3.2.Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie: _____lei MD.

(suma cu cifre şi litere)

3.3. Metoda şi condiţiile de plată de către Cumpărător vor fi: *Achitarea va fi efectuată prin transfer, pe contul Vînzatorului, timp de 15 zile din data livrării bunurilor semnăriii facturii fiscale şi Actului de instalare* ***Anexa nr.3. (pentru Lotul 1)***

3.4 Plăţile se vor efectua prin transfer bancar pe contul de decontare al Vînzătorului indicat în prezentul Contract.

4. Condiţii de predare-primire

4.1. Bunurile se consideră predate de către Vînzător şi recepţionate de către Cumpărător dacă:

a) cantitatea Bunurilor corespunde Specificaţiei tehnice ***Anexa nr.1***și Specificaţiei de preț ***Anexa nr.2*** și informaţiei indicate în documentele de însoţire conform punctului 2.2 al prezentului Contract;

b) calitatea Bunurilor corespunde informaţiei indicate în Specificaţia tehnică ***Anexa nr.1*** și în Partea II ”Condițiile speciale a contractului”;

c) bunurile sunt instalate și funcționale cu întocmirea *Actului instalare* ***Anexa nr.3 (pentru Lotul 1)*** și semnat de ambele părți.

4.2. Vînzătorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plăţii. Pentru nerespectarea de către Vînzător a prezentei clauze, Cumpărătorul își rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.3 corespunzător numărului de zile de întîrziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.3.

5. Standarde

5.1. Produsele furnizate în baza contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Vînzătorul se obligă:

a) să livreze Bunurile în condiţiile prevăzute în Specificaţia tehnică din ***Anexa nr.1***.

b) să anunţe Cumpărătorul după semnarea prezentului Contract, în decurs de __5__ zile calendaristice, prin telefon/fax sau poșta electronică achizitiicnas@cnas.gov.md, despre disponibilitatea livrării Bunurilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Bunurilor de către Cumpărător , în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Bunurilor pe toată perioada de până la recepţionarea lor de către Cumpărător.

6.2. În baza prezentului Contract, Cumpărătorul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Bunurilor livrate în corespundere cu cerinţele prezentului Contract;

b) să asigure achitarea Bunurilor livrate, respectînd modalităţile şi termenele indicate în prezentul Contract.

7. Circumstanțe care justifică neexecutarea contractului

7.1. Părţile sunt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanțe care

justifică neexecutarea contractului (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).
7.2. Partea care invocă clauza circumstanțelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor care justifică neexecutarea contractului.
7.3. Survenirea circumstanţelor care justifică neexecutarea contractului, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.
7.4 În cazul în care în circumstanțele care justifică neexecutarea contractului, acesta se modifică prin acordul adițional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct.7.1 și pct. 7.3, părțile modifică contractul prin acord - adițional, privind neîndeplinerea parțială sau integrală a obligațiunilor, inclusiv modificarea termenilor în cazul suspendării și executării ulterioare a contractului.

8. Rezoluțiunea

8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părţilor.
8.2. Contractul poate fi rezolvit în mod unilateral de către:
a) Cumpărător în caz de refuz al Vînzătorului de a livra Bunurile prevăzute în prezentul Contract;
b) Cumpărător în caz de nerespectare de către Vînzător a termenelor de livrare stabilite;
c) Vînzător în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;
d) Vînzător sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.
8.3 Cumpărătorul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situaţii:
a) contractantul se afla, la momentul atribuirii lui, în una dintre situaţiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art. 19 al Legii nr.131/2015 privind achizițiile publice;
b) contractul a făcut obiectul unei modificări substanțiale care necesita o nouă procedură de achiziție publică în conformitate cu art. 76 al Legii nr.131/2015 privind achizițiile publice;
c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, avînd în vedere o încălcare gravă a obligaţiilor ce rezultă din Legea nr.131/2015 privind achizițiile publice și/sau tratatele internaţionale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanțe judecătorești naționale sau, după caz, internaționale.
8.4. Partea iniţiatoare a rezoluțiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.
8.5. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniția rezoluțiunea.

9. Reclamaţii

9.1. Reclamaţiile privind cantitatea Bunurilor livrate sunt înaintate Vînzătorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vînzătorului.
9.2. Pretenţiile privind calitatea bunurilor livrate sunt înaintate Vînzătorului în termen de 5 zile de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.
9.3. Vînzătorului este obligat să examineze pretenţiile înaintate în termen de 3 zile de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.
9.4. În caz de recunoaştere a pretenţiilor, Vînzătorului este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.
9.5. Vînzătorul poartă răspundere pentru calitatea Bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.
9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întîrziere sunt

suportate de partea vinovată.

10. Sancţiuni

10.1. Pentru refuzul de a vinde Bunurile prevăzute în prezentul Contract, se va reține o penalitate în valoare de 5% din suma totală a contractului.
10.2. Pentru livrarea cu întârziere a Bunurilor, Vînzătorul poartă plata despăgubirei în valoare de 0,1% din suma Bunurilor nelivrate, pentru fiecare zi de întârziere, dar nu mai mult de 5 % din suma totală a prezentului Contract. În cazul în care întârzierea depășește 15 zile, se consideră ca fiind refuz de a livra Bunurile prevăzute în prezentul Contract și Vînzătorului i se va reține o penalitate în valoare de 5% din suma totală a contractului în conformitate cu prevederile pct.10.1.
10.3. Pentru achitarea cu întârziere, Cumpărătorul poartă plata despăgubirei în valoare de 0,1% din suma Bunurilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 5% din suma totală a prezentului contract.
10.4. Prima zi lucrătoare ulterioară datei ce constituie termenul limită de livrare, precum și, termenul limită de achitare se consideră zi lucrătoare de întârziere.
10.5. Suma penalităţii calculate Vînzătorului conform prezentului Contract poate fi dedusă (reţinută) de către Cumpărător din suma plăţii pentru Bunurile livrate.

11. Drepturi de proprietate intelectuală

11.1. Vînzătorul are obligaţia să despăgubească beneficiarul împotriva oricăror:
a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru sau în legătură cu produsele achiziţionate, şi
b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor

12. Dispoziţii finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.
12.2. Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.
12.3. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.
12.4. Prezentul Contract în cazul în care este semnat electronic, de către ambele părți, acesta este remis în mod automat prin mijloacele electronice, dar în cazul când contractul este semnat olografic se întocmește în două exemplare în limba română, câte un exemplar pentru Vînzător și Cumpărător.
12.5. Prezentul contract este valabil până la **31.12.2025.**
12.6. Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova.

II. CONDIȚIILE SPECIALE A CONTRACTULUI

1. Garanția echipamentelor livrate cade în răspunderea Vânzătorului pe toată perioada de garanție care constituie 12 luni.
2. În caz de defecție a echipamentului furnizorul trebuie să asigure repararea elementelor defectate sau să dețină rezerve necesare pentru substituire lor în baza garanției. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează

la sediul Aparatului Central CNAS.

3. Bunurile vor fi livrate cu transportul Vânzătorului și descărcate în depozitul Aparatului Central al CNAS mun. Chișinău, str. Gh. Tudor 3.
4. Bunurile livrate urmează să fie însoțite de certificatul de origine și certificatul de atestare a calității echipamentului.
5. Bunurile livrate urmează să fie noi (non refurbished), iar data producerii să nu fie mai veche de un an de la data livrării.
6. Ofertantul va prezenta Autorizare(MAF) de la producător, actul care atestă dreptul oficial al reprezentantului pe teritoriul R. Moldova de a livra bunuri/lucrări/servicii.
7. Pentru Lotul 1 va prezenta Certificat al inginerului tehnic din cadrul companiei ofertante pe produsul ofertat și inclusiv certificatul Cisco Certified Network Associate Routing and Switching sau echivalentul.
8. Pentru Lotul 1 va fi executate serviciile de instalarea, configurarea și darea in exploatare a produsului ofertat, inclusiv transferul de cunoștințe către Cumpărător, pentru a permite celor instruiți să preia menținerea și configurarea ulterioară a echipamentului ofertat, în conformitate cu necesitățile.

RECHIZITELE JURIDICE, POŞTALE ŞI DE PLĂŢI ALE PĂRŢILOR

Prestatorul	**Beneficiarul**
	Casa Naţională de Asigurări Sociale
Adresa poştală:	Adresa poştală: *mun. Chişinău,* str. *Gh. Tudor,№3*
Telefon:	Telefon: (022)25-75-51
Banca:	Ministerul Finanţelor, Trezoreria de Stat
Cod Bancar:	Cod Bancar: TREZMD2X
IBAN:	IBAN: MD84TRPFAH518710AO1691AA
Cod fiscal:	Cod fiscal: *1004600030235*

SEMNĂTURILE PĂRŢILOR

“Vînzător”:	**“ Cumpărător”:**
	Directoare generală Elena ȚÎBÎRNĂ
L.Ş.	L.Ş.

Anexa nr. 1
la contractul nr. _____
Din „____” _____ 20_____

SPECIFICAŢII TEHNICE –

№	Denumirea bunului	Specificarea tehnică deplină solicitată		Unitatea de măsură	Cantitate
1.	**Lotul nr. 1**				
1	***Router***	**Caracteristica**	**Cerinte tehnice**	**bucăți**	**1**
		Type			
		Throughput: Threat Defense Software			
		IPS Throughput			
		Interfaces			
		Throughput: Firewall (FW) + Application Visibility and Control (AVC) (1024B)			
		Throughput: FW + AVC + Intrusion Prevention System (IPS) (1024B)			
		Maximum concurrent sessions, with AVC			
		Maximum new connections per second, with AVC			
		Transport Layer Security (TLS)			
		IPSec VPN throughput (1024B TCP w/Fastpath)			

		Maximum VPN Peers			
		Device Manager (local management)			
		Centralized management			
		AVC			
		Open-source application detectors			
		Security Intelligence			
		IPS			
		Malware Defense for Networks			
		Malware Analytics sandboxing			
		URL filtering: number of categories			
		URL filtering: number of URLs categorized			
		Automated threat feed and IPS signature updates			
		Stateful inspection firewall throughput1			
		Stateful inspection firewall throughput (multiprotocol)2			
		Concurrent firewall connections			
		New connections per second			
		IPsec VPN throughput (450B UDP L2L test)			
		Maximum VPN Peers			

		Security contexts (included; maximum)			
		High availability			
		High availability and clustering			
		Scalability			
		Adaptive Security Device Manager			
		Form factor (rack units)			
		Integrated I/O, min			
		Integrated network management ports			
		Serial port			
		USB, min			
		Storage, min			
		Power supply configuration			
		AC input voltage			
		AC maximum input current			
		AC maximum output power			
		AC frequency			
		AC efficiency			
		Fans			
		Noise			
		Rack mountable			
		Humidity: operating			
		Humidity: nonoperating			
		Regulatory compliance			
		Safety			
		EMC: emissions			
		EMC: immunity			
2	***Echipamentul firewall de generație următoare (NGFW)***	- 1. Protecția rețelei cu controlul stării sesiunilor; - 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile			

		care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; - 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. - 4. Firewall-ul NGFW propus nu trebuie să necesite o repornire pentru a verifica și instala actualizările de securitate. - 5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite. - 6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor. - 7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea). - 8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. - 9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas. - 10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere. - 11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS. - 12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele. - 13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale. - 14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne. - 15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o		

		politică unică de securitate. - 16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe. - 17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații: - 17.1 . Aplicații corporative: - 17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS; - 17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase; - 17.1.3. Servicii de fișiere, inclusiv Microsoft SMB. - 17.1.4. ERP, CRM, inclusiv SAP, 1C; - 17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; - 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; - 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; - 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; - 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; - 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; - 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; - 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; - 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; - 17.2. Aplicații Internet: - 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; - 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте,		

		Odnoklassniki, „Moy Mir”; - 17.2.3. Servicii de mesagerie instantanee, inclusiv ICQ, Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; - 17.2.4. Servicii de conferință audio-video, inclusiv Skype; - 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav; - 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; - 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; - 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; - 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; - 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodoare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; - 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; - 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; - 21. Inspecția tunelurilor: - 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); - 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; - 21.3. Mod de transport AH IPSec. - 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune;		

		- 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; - 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; - 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: - 25.1. Adresa IP a expeditorului, - 25.2. Adresa IP a destinatarului, - 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, - 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, - 25.5. Aplicațiile la nivelul 7 al modelului OSI, - 25.6. URL categorii. - 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni: - • Permisiune sau interdicție; - • Permisiunea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi		

		TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni; - • Permisiune, dar cu scanare pentru viruși și alte amenințări; - • Permisiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; - • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; - • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; - • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; - • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; - • Aplicarea redirecționării traficului pe bază de politici (Policy Based Forwarding); - • Permisiunea anumitor funcții ale aplicației; - • Oricare combinație dintre acțiunile de mai sus. - 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; - 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; - 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; - 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; - 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări;		

		- 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; - 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); - 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; - 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; - 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; - 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; - 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; - 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2003, 2007 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; - 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; - 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; - 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului		

		pentru verificare; - 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; - 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; - 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. - 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. - 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. - 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; - 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; - 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; - 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; - 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; - 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare;		

		- 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; - 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; - 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare):Duo, - • Okta, - • RSA SecureID, - • PingID; - 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); - 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; - 59. Funcționalitate de protecție împotriva atacurilor DoS; - 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; - 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; - 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; - 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la: Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; - 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. - 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. - 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru		

		firewall-uri de același furnizor. - - 67. Cerințe pentru sistemul de management centralizat: - • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; - • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); - • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; - • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. - • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. - • Platforma trebuie să suporte gestionarea a cel puțin 1000 de echipamente firewall de nouă generație (NGFW); - • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; - • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; - • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; - • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme.		

		- • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; - • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. - • Platforma trebuie să permită organizarea echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; - • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); - 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. - 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. - 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. - 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. - 72. Funcționalitatea IPSec VPN. - 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. - 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. - 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). - 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. - 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. - 78. Suport pentru rutarea între VLAN-uri. - 79. Suport pentru NAT, DHCP și DHCP relay. - 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). - 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). - 82. Suport pentru pachete mari (Jumbo frames). - - 83. Managementul rolurilor administratorilor locali: - • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul		

		dispozitivului și al sistemelor virtuale (contexte); - • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; - • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. - - 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. - Cerințe de performanță ale firewall-ului: - Performance: - • Threat prevention throughput 0.8 Gbps; - • IPsec VPN throughput 650 Mbps; - • Connections per second 1100; - • Firewall throughput 1.4 Gbps; - • Max sessions (IPv4 or IPv6) 64,000. - - Policies: - • Security rules 500; - • Security rule schedules 256; - • NAT rules 400; - • Decryption rules 100; - • App override rules 100; - • Tunnel content inspection rules 100; - • SD-WAN rules 100; - • Policy based forwarding rules 100; - • Captive portal rules 10; - • DoS protection rules 100. - - Security Zones: - • Max security zones 25. - - Objects (addresses and services): - • Address objects 2500; - • Address groups 125;		

		- • Members per address group 2,500; - • Service objects 1,000; - • Service groups 250; - • Members per service group 500; - • FQDN address objects 2,000; - • Max DAG IP addresses 1000; - • Tags per IP address 32. - - Security Profiles: - • Security profiles 75. - SSL Decryption: - • Max SSL inbound certificates 25; - • Max concurrent decryption sessions 6600; - URL Filtering: - • Total entries for allow list, block list and custom categories 25,000; - • Max custom categories 2,849; - • Max custom categories (virtual system specific) 500; - Interfaces: - • I/O: 1G RJ45 (7); - • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2). - - Storage Capacity: - • 64 GB eMMC - Virtual Routers: - • Virtual routers 3. - Routing: - • IPv4 forwarding table size 5,000; - • IPv6 forwarding table size 2500; - • System total forwarding table size 5,000; - • Max routing peers (protocol dependent) 500; - • Static entries - DNS proxy 1,024. - L2 Forwarding: - • ARP table size per device 1500; - • IPv6 neighbor table size 1500; - • MAC table size per device 1500; - • Max ARP entries per broadcast domain 1500; - • Max MAC entries per broadcast domain 1500. - NAT: - • Total NAT rule capacity 400; - • Max NAT rules (static) 400; - • Max NAT rules (DIP) 400; - • Max NAT rules (DIPP) 200; - • Max translated IPs (DIP) 16000;		

		- • Max translated IPs (DIPP) 200. - Address Assignment: - • DHCP servers 3; - • DHCP relays 500; - • Max number of assigned addresses 64,000. - High Availability: - • Devices supported 2; - • Max virtual addresses 32. - QoS: - • Number of QoS policies 1,000; - • Physical interfaces supporting QoS 8; - • Clear text nodes per physical interface 31. - IPSec VPN: - • Max IKE Peers 1000; - • Site to site (with proxy id) 1000; • SD-WAN IPsec tunnels 1000. **Termen de garanție – 12 luni**;		

SEMNĂTURILE PĂRŢILOR

Vînzătorul

L.Ș.

Cumpărătorul

Directoare generală Elena ȚÎBÎRNĂ

L.Ș.

Anexa nr. 2
la contractul nr._____
din "____" _____ 20___

SPECIFICAŢII DE PREŢ –

№	Specificarea tehnică deplină solicitată	Cantitate bucăți	Preţ unitar fără TVA	Preţ unitar cu TVA	Suma fără TVA	Suma cu TVA
	Lotul nr. 1					
1	***Router***	**1**				
	Lotul nr. 2					
2.	**Echipamentul firewall de generație următoare (NGFW)**	**5**				
Suma totală fără TVA lei MD						
Suma totală cu TVA lei MD						

SEMNĂTURILE PĂRŢILOR

Vînzătorul

Cumpărătorul

Directoare generală Elena ȚÎBÎRNĂ

L.Ș.

L.Ș.

Anexa nr.3
la Contractul nr.___
din _ _____ 20___

Model Act instalare (pentru Lotul nr. 1)

Act instalare

<<____>>_____2024

Persoana responsabilă **Nume,prenume**	
Echipa de montare.	

Serviciul prestat

_____ _____
(Vânzător) (persoana responsabilă din partea Vânzătorului)

_____ _____
(Cumpărător) (Am primit)

“Vânzător”: _____ L.Ş.	**“Cumpărător”:** **Directoare generală Elena ȚÎBÎRNĂ** _____ L.Ş.