ACHIZIŢII PUBLICE

CONTRACT nr. 54 LP
de achiziţionare a bunurilor

Cod CPV: **48000000-8**

16 octombrie 2018 **mun. Chişinău**

Furnizorul de bunuri / Prestatorul de servicii	**Autoritatea contractantă**
Î.C.S. „RELIABLE SOLUTIONS DISTRIBUTOR" SRL	**ADMINISTRAŢIA NAŢIONALĂ A PENITENCIARELOR**
reprezentată prin Viorica ODOBESCU	reprezentată prin Serghei DEMCENCO
care acţionează în baza statutului	care acţionează în baza regulamentului
denumit(a) în continuare *Vânzător/prestator,*	denumit(a) în continuare *Cumpărător/ beneficiar, 1006601001012*
nr. 1010600010328 din 30.03.2010	
pe de o parte,	pe de altă parte,

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

a. Achiziţionarea **„Pachetelor Software şi sisteme informatice"** denumite în continuare Bunuri (şi/sau Servicii), conform **LP *nr.18/04041 din 05 octombrie 2018***, în baza deciziei grupului de lucru al Administraţiei Naţionale a Penitenciarelor, nr. **18/*04041/001* din 11 octombrie 2018.**

b. Următoarele documente vor fi considerate părţi componente şi integrale ale Contractului:

a) Formularul contractului;
b) Specificaţia preţ;
c) Lista bunurilor/serviciilor şi graficul livrării/prestării;
d) Garanţie de bună execuţie.

c. Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

Digitally signed by Creangă Ovidiu-Vincenzo
Date: 2020.12.30 15:38:36 EET
Reason: MoldSign Signature
Location: Moldova

d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător/beneficiar, Vânzătorul/prestatorul se obligă prin prezenta să livreze Cumpărătorului/beneficiarului Bunurile şi/sau Serviciile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e. Cumpărătorul/beneficiarul se obligă prin prezenta să plătească Vânzătorului/prestatorului, în calitate de contravaloare a livrării bunurilor şi serviciilor, precum şi a înlăturării defectelor lor, preţul Contractului sau orice altă sumă care poate deveni plătibilă conform prevederilor Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1. Vânzătorul/prestatorul îşi asumă obligaţia de a livra Bunurile şi/sau de a presta Serviciile conform Specificaţiei, care este parte integrantă a prezentului Contract.

1.2. Cumpărătorul/beneficiarul se obligă, la rândul său, să achite şi să recepţioneze Bunurile şi/sau Serviciile livrate de Vânzător.

1.3. Calitatea Bunurilor şi/sau a Serviciilor se atestă prin certificatele de calitate indicate în Specificaţie. Bunurile livrate şi/sau Serviciile prestate în baza contractului vor respecta standardele indicate în Specificaţie. Când nu este menţionat nici un standard sau reglementare aplicabilă, se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

1.4. Termenele de garanţie *[valabilitate, după caz]* a Bunurilor şi/sau Serviciilor sunt indicate în Specificaţie.

2. Termenele şi condiţiile de livrare / prestare

2.1. Livrarea Bunurilor şi/sau prestarea Serviciilor se efectuează de către Vânzător conform anexei nr. 1 şi în termenele prevăzute de graficul de livrare conform anexei nr.2.

2.2. În caz de necesitate, cumpărătorul îşi rezervă dreptul să instituie grafice de livrare suplimentare, cu modificarea cantităţilor stabilite pentru fiecare penitenciar în parte.

2.3. Documentaţia de însoţire a Bunurilor şi/sau a Serviciilor include:

a) Originalele facturilor fiscale;

2.4. Originalele documentelor prevăzute în punctul 2.3 se vor prezenta Cumpărătorului cel târziu la momentul livrării bunurilor la destinaţia finală. Livrarea produselor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. Preţul Contractului şi condiţiile de plată

3.1. Preţul Bunurilor şi/sau a Serviciilor livrate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat în Specificaţia prezentului Contract *(anexa nr.1)*.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie **lei 00 bani MD, inclusiv TVA.**

3.3. Achitarea plăţilor pentru Bunurile livrate şi/sau Serviciile prestate se va efectua în lei moldoveneşti *(anexa nr.2)*.

3.4. Metoda şi condiţiile de plată de către Cumpărător vor fi: *se efectuează în termen de 30 zile după livrare (prestare) a bunurilor, în baza facturii fiscale.*

3.5 Plăţile se vor efectua prin transfer bancar pe contul de decontare al Vânzătorului indicat în prezentul Contract. În acest scop, Cumpărătorul se obligă să emită Ordinul de plată (transfer) şi să-l înainteze spre achitare Trezoreriei, acesta constituind momentul de executare a plăţii.

4. Condiţiile de predare-primire

4.1. Bunurile şi/sau Serviciile se consideră predate de către Vânzător şi recepţionate de către Cumpărător *[destinatar, după caz]* dacă:

a) cantitatea Bunurilor şi/sau a Serviciilor corespunde informaţiei indicate în Lista bunurilor / serviciilor şi graficul livrării / prestării şi documentele de însoţire conform punctului 2 al prezentului Contract;

b) calitatea Bunurilor şi/sau a Serviciilor corespunde informaţiei indicate în Specificaţie;

c) ambalajul şi integritatea Bunurilor corespunde informaţiei indicate în Specificaţie.

4.2. Vânzătorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor şi/sau prestarea Serviciilor, pentru efectuarea plăţii. Pentru nerespectarea de către Vânzător a prezentei clauze, Cumpărătorul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întârziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.4.

5. Standarde

5.1 Produsele furnizate în baza contractului vor respecta standardele prezentate de către furnizor în propunerea sa tehnică.

5.2 Când nu este menţionat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Vânzătorul se obligă:

a) să livreze Bunurile şi/sau să presteze Serviciile în condiţiile prevăzute de prezentul Contract;

b) să anunţe Cumpărătorul după semnarea prezentului Contract, în decurs de 5 zile calendaristice, prin telefon/fax sau telegramă autorizată, despre disponibilitatea livrării Bunurilor şi/sau prestării Serviciilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Bunurilor şi/sau Serviciilor de către Cumpărător *[destinatar, după caz]*, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Bunurilor şi/sau Serviciilor pe toată perioada de până la recepţionarea lor de către Cumpărător *[destinatar, după caz]*.

6.2. În baza prezentului Contract, Cumpărătorul se obligă:

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

b) să asigure achitarea Bunurilor livrate şi/sau Serviciilor prestate, respectând modalităţile şi termenele indicate în prezentul Contract.

7. Forţa majoră

7.1 Părţile sânt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de forţă majoră (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2 Partea care invocă clauza de forţă majoră este obligată să informeze imediat (dar nu mai târziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor de forţă majoră.

7.3 Survenirea circumstanţelor de forţă majoră, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un certificat, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.

8. Rezilierea

8.1 Rezilierea Contractului se poate realiza cu acordul comun al Părţilor.

8.2 Contractul poate fi reziliat în mod unilateral de către:

a) Cumpărător în caz de refuz al Vînzătorului de a livra Bunurile şi/sau de a presta Serviciile prevăzute în prezentul Contract;

b) Cumpărător în caz de nerespectare de către Vînzător a termenelor de livrare/prestare stabilite;

c) Vînzător în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor / Serviciilor;

d) Vînzător sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.

8.3 Partea iniţiatoare a rezilierii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.

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 iniţia rezilierea.

9. Reclamaţii

9.1 Reclamaţiile privind cantitatea Bunurilor livrate sau Serviciilor prestate sînt înaintate Vînzătorului/Prestatorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vînzătorului/Prestatorului.

9.2 Pretenţiile privind calitatea bunurilor şi/sau serviciilor livrate sînt înaintate Vînzătorului în termen de 5 zile lucrătoare 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 Vînzătorul este obligat să examineze pretenţiile înaintate în termen de 5 zile lucrătoare de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.

9.4 În caz de recunoaştere a pretenţiilor, Vînzătorul este obligat, în termen de 5 zile, să livreze/presteze suplimentar Cumpărătorului cantitatea nelivrată de bunuri şi/sau serviciile neprestate, 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 şi/sau a Serviciilor 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 sînt suportate de partea vinovată.

10. Sancţiuni

10.1. Forma de garanţie de bună executare a contractului agreată de Cumpărător

este **7 044,00 (şapte mii patruzeci şi patru) lei 00 bani,** în cuantum de 5% din valoarea contractului.

10.2. Pentru refuzul de a vinde Bunurile şi/sau de a presta Serviciile prevăzute în prezentul Contract, se va reţine garanţia de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevederile punctului 10.1., în caz contrar Vânzătorul suportă o penalitate în valoare de 5% din suma totală a contractului.

10.3. Pentru livrarea/prestarea cu întârziere a Bunurilor/Serviciilor, Vânzătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor nelivrate şi/sau a Serviciilor neprestate, pentru fiecare zi de întârziere, dar nu mai mult de 5 % din suma totală a prezentului Contract. În cazul în care întârzierea depăşeşte 5 zile, se consideră ca fiind refuz de a vinde Bunurile şi/sau de a presta Serviciile Prevăzute în prezentul Contract şi Vânzătorul i se reţine garanţia de bună executare a contractului, în cazul în care ea fost constituită în conformitate cu prevederile punctului 10.1.

10.4. Pentru achitarea cu întârziere, Cumpărătorul poartă răspundere materială în valoare de 0,1 % din suma Bunurilor şi/sau a Serviciilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 5 % din suma totală a prezentului contract.

11. Drepturi de proprietate intelectuală

11.1 Furnizorul are obligaţia să despăgubească achizitorul 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

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 De la data semnării prezentului Contract, toate negocierile purtate şi documentele perfectate anterior îşi pierd valabilitatea.

12.3 Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin act 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.

12.4 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.

12.5 Prezentul Contract este întocmit în trei exemplare în limba de stat a Republicii Moldova, cîte un exemplar pentru Vînzător, Cumpărător şi Agenţia Achiziţii Publice.

12.6 Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare după înregistrarea lui de către Agenţia Achiziţii Publice şi, după caz , de către Trezoreria de Stat sau de către una din trezoreriile teritoriale ale Ministerului Finanţelor, fiind valabil pînă la **31 decembrie 2018**.

12.7 Prezentul Contract reprezintă acordul de voinţă al ambelor părţi şi este

semnat astăzi, „ ” octombrie 2018.

12.8 Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova, la data şi anul indicate mai sus.

Datele juridice, poştale şi bancare ale Părţilor:	
Vânzătorul/Prestatorul	**Cumpărătorul/Beneficiarul**
Î.C.S. „RELIABLE SOLUTIONS DISTRIBUTOR” SRL	**ADMINISTRAŢIA NAŢIONALĂ A PENITENCIARELOR**
mun.Chişinău, str. Alexandru cel Bun, 85	or. Chişinău, str. Titulescu, 35
Telefon: 022 210 208; fax: 022 223 963	Telefon: 022 409-714, fax: 409-709
Cod IBAN: MD31EX0000002251697722MD	Cont de plăţi: 226301
B.C. „Eximbank” S.A.	Prestatorul plătitor: Ministerul Finanţelor - Trezoreria de Stat
Adresa poştală a băncii: mun. Chişinău, bd. Grigore Vieru, 16, Sucursala nr.9	Adresa poştală a băncii: mun. Chişinău
Cod banca: EXMMMD22	Cod bancar: TREZMD2X
Cod fiscal: 1010600010328	Cod fiscal: 1006601001012
Cod TVA: 0207778	Cont trezorerial: 317110D00792AC 314110D00792AC
	Cod IBAN: MD19TRPBAA317110D00792AC - 111.000,00 lei
	MD44TRPBAA314110D00792AC - 29.880,00 lei
Semnăturile părţilor	
Semnătura autorizată:	
Viorica ODOBESCU	**Serghei DEMCENCO**
L.Ş.	L.Ş.
DF	
DJ:	
	Înregistrat: nr.
	Trezoreria
	Data: 30. OCT. 2018

2018-000001852

Anexa nr. 1
la contractul nr. 54 LP
din 16 octombrie 2018

SPECIFICAŢIA BUNURILOR (SERVICIILOR)

Nr. d/o	Denumirea bunului	Cantitatea	Preţ(lei) metri/buc		Suma totală (lei)		Termen şi locul de livrare
			Fără TVA	Cu TVA	Fără TVA	Cu TVA	
1.	**Licenţă Antivirus (echivalent McAfee Endpoint Protection)**	**200 buc.**	**200,00**				Octombrie – 15 Decembrie mun.Chişinău, str.Tituleascu,35
	Producător –**"McAfee"**; Ţara de origine – **SUA**						
2.	**Soluţie software pentru protecţia împotriva scurgerii de informaţii (DLP – Data Loss Prevention)**	**50 buc.**					
	Producător –**"McAfee"**; Ţara de origine – **SUA**						
3.	**Server „Maguay eXpertServer"**	**1 buc.**					
	Producător –**„Maguay"**; Ţara de origine – **R omânia.**						
Suma totală:							

Specificaţia tehnică:

Lotul 1. Licenţă Antivirus (echivalent McAfee Endpoint Protection) :

Modelul articolului – McAfee Endpoint Threat Protection with 1year of support;
Ţara de origine – SUA;
Producătorul – McAfee.

1. Trebuie sa asigure protecţie pentru staţii de lucru si servere cu următoarele sisteme de operare:
Windows 10 Versiunile 1507, 1511, 1607, 1703;Windows 10 IoT Enterprise;Windows 8.1, Update 1, August 2014 update rollup;Windows 8 (Win NT 6.2) Editions: Basic / Pro / Enterprise;Windows 7 (Home Premium / Professional / Ultimate / Enterprise);Windows Vista;Windows Vista Business/Ultimate for Embedded Systems;Windows 7 Professional/Ultimate for Embedded Systems;Windows Server 2016 Editions: Datacenter / Essentials / Standard installed in „Server with Desktop Experience" mode;Windows Server 2012 Release 2 (R2) , R2 Update 1, R2 August 2014 update;Windows Server 2008, HyperV, Standard, Datacenter, Enterprise, Foundation, Web, HPC;VMware ESX, ESXi

2. Integrare cu serviciile de directoare, precum Microsoft AD şi Open LDAP;

3. Soluţia trebuie sa ofere protecţie pentru staţii de lucru si servere cu roluri precum Windows Active Directory Domain Controller, Microsoft SQL server, Microsoft Exchange Server, fără impact negativ;

4. Instalarea centralizată pe staţii de lucru, servere şi a aplicaţiilor terţe

5. Dezinstalarea agentului/modulelor în mod centralizat sau în urma unui mecanism de tipul solicitare/acceptare;

6. Compatibilitate, la nivelul nodurilor endpoint, între soluţiile de tip Endpoint Protection şi DLP, prin folosirea unui singur agent, în scop de minimizare resurse, precum integrarea şi cu alte soluţii implementate în cadrul instituţiei, precum soluţii de tip accounting, encryption, chat/messenger, ş.a. (compatibilitate determinată la etapa de testare a soluţiilor preselectate); Agentul unic să poată fi instalat în mod silenţios, fără alertarea utilizatorului;

7. Produsul oferta trebuie sa permită integrarea şi managementul şi altor aplicaţii/echipamente de Securitate precum: (antivirus, prevenirea scurgerilor de date, log management, controlul traficului de tip mail si web, protecţia bazelor de date) toate gestionata cu o consola unica pentru a unifica administrarea acestora si a uniformiza tehnologiile;
Cerinţe fata de consola de management:

8. Crearea/aplicarea politicilor de securitate pentru utilizatori/sisteme în parte şi pentru grupuri de utilizatori/sisteme, în funcţie de regulile prestabilite;

9. Automatizarea sarcinilor de instalare/dezinstalare a componentelor endpoint (agenţi, module), de generare a rapoartelor şi de transmitere a notificărilor prin email;

10. Automatizarea sarcinilor de atribuire a politicilor de securitate pe nodurile endpoint (staţii de lucru, servere, dispozitive mobile, atm-uri) în funcţie de specificaţiile sistemului de operare;

11. Crearea de roluri pentru administratori, auditori, supervizori, ofiţeri de securitate, ş.a.;

12. Crearea de notificări pe email (alerte) personalizate, în dependență de tipul evenimentului înregistrat și sursa acestuia;
13. Generarea rapoartelor detaliate despre sistemele administrate și despre evenimentele generate de acestea, precum și despre sistemele neadministrate din rețea;
14. Generarea rapoartelor care va permite agregarea evenimentelor generate de Componența de prevenire a intruziunilor pe categorii precum: nume sistem, ip sursa atacator, ip destinație atac, nume amenințare, categorie amenințare, factor de risc, grupare logica in consola;
15. Personalizarea rapoartelor cu text și logo-ul instituției, cu tabele, grafice, liste, sumare;

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

16. Salvarea rapoartelor, trimiterea prin e-mail, exportarea în format pdf/csv/html, exportarea într-un format arhivat și expedierea automată pe e-mail către destinatarii prestabiliți;
17. Va dispune de o unealta care sa permită colectarea automata a logurilor și a altor informații necesare pentru deschiderea unui caz de suport;
18. Va permite pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți si instalarea acestora pe stațiile de lucru;
19. Va oferi instalarea și administrarea componentelor antivirus, web control, threat detection, firewall, prevenire a intruziunilor, de control al dispozitivelor externe, de control al aplicațiilor, de DLP și etichetare și clasificare si criptare trebuie să se facă dintr-o singură consolă;
20. Consola trebuie sa poate fi instalată în mediu Microsoft Cluster de tip activ/pasiv;
21. Acțiunile utilizatorilor în consolă să fie posibil de supus auditului;
22. Componența ce asigură canalul de comunicație criptat dintre server și stații de lucru trebuie să fie validată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.);
23. Consola trebuie să folosească un propriu index pentru a identifica și actualiza datele despre sistemele care își schimbă proprietăți precum nume,ip și configurație hardware;
24. Consola trebuie să poată fi instalată pe o mașină fizică sau virtuală cu următoarele caracteristici fizice minime:
25. Sistem de operare: Server Windows 2016, Server Windows 2012 Release 2 (R2), Server Windows 2012, Server Windows 2008 cu SP2 64-bit (Standard, Enterprise sau Datacenter), Server Windows 2008 R2 64-bit (Standard, Enterprise, or Datacenter);
26. Server virtual: VMware ESX/ESXi 5.x sau mai recent, Citrix XenServer 6.0, Citrix XenServer 5.5 Update 2, Windows Server 2012 Hyper-V, Windows Server 2008 R2 Hyper-V sau mai noi;
27. Baza de date: Server SQL 2016, Server SQL 2016 Express, Server SQL 2014, Server SQL 2014 Express, Server SQL 2012 Express, Server SQL 2012, Server SQL 2008 with SP1/SP2/R2 Standard, Enterprise, Workgroup, Express;
28. Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe:
29. Sisteme individuale
30. Grupuri de sisteme
31. Sisteme din AD;
Cerințe generale față de Soluția Endpoint protection solicitată
32. Impact minim (sub 10%) asupra performanțelor sistemului endpoint pe care este instalat (impact determinat la etapa de testare a soluțiilor preselectate);
33. Soluția trebuie sa vina cu o unealta de monitorizare a consumului de resurse ce generează rapoarte pe baza cărora se pot face optimizări;
34. Soluția trebuie să permită optimizarea consumului de resurse prin configurarea de politici de scanare diferite în funcție de aplicații;
35. Soluția trebuie să permită alocarea dinamică a resurselor pe endpoint, pentru optimizarea de performanțe;
36. Actualizarea semnăturilor trebuie să se facă incremental pentru a evita încărcarea rețelei;
37. Soluția trebuie sa folosească un singur motor de scanare a antivirusului de stație, pentru a nu se încărca suplimentar memoria sistemelor de calcul;
38. Aplicarea politicilor de securitate chiar și atunci când nodul endpoint nu este conectat la rețeaua instituției, cu posibilitatea de a aplica politici specifice pentru astfel de situații;
39. Criptarea canalului de comunicație dintre serverul de administrare și nodurile endpoint;
40. Criptarea canalului de comunicație pentru accesarea consolei de administrare;
41. Importul de certificate digitale eliberate de o autoritate autorizată sau generate pe intern;
42. Posibilitatea configurării intervalului de sincronizare între serverul de administrare și componentele endpoint (agenți, module);
43. Detectarea în rețea a sistemelor noi apărute (neînregistrate în consola de administrare);
44. Nivelul de protecție similar și în mediul de operare Windows SafeMode;
45. Păstrarea criptată a evidențelor/evenimentelor de securitate pe serverul de administrare;
46. Jurnalizarea (logarea) evenimentelor și funcționalităților la nivelul agenților/modulelor endpoint și serverelor/consolelor de administrare, cu transmiterea logurilor în regim real prin intermediul protocolului Syslog.

47. Protecție antivirus, antispam, antispyware, antimalware, antiphishing, antirootkit, adware, dialers, password crackers, key loggers, firewall pentru stații de lucru, laptop-uri, servere fizice și virtualizate;
48. Scanarea și identificarea aplicațiilor/codurilor malițioase utilizând o bază de date cu semnături, analiză euristică și pe bază de reputație;
49. Aplicarea regulilor de reacționare în timpul producerii unui eveniment de securitate: identificare, blocare, dezinfectare, eliminare, mutare în carantină, notificare, înregistrare a evidențelor;
50. Actualizarea (automată) a definițiilor/semnăturilor antivirus, precum și offline prin instalarea manuală a unor pachete descărcate;

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

51. Scanarea suporturilor externe de stocare (dispozitive USB, CD/DVD) în momentul imediat conectării acestora, pentru a identifica și elimina amenințările în mod proactiv;
52. Capabilități de firewall local cu funcții de filtrare a pachetelor și blocare la nivel aplicație;
53. Scanarea și protecția resurselor partajate în rețea;
54. Soluția sa nu poată fi oprita de utilizator chiar daca acesta are dreptul de administrator local;
55. Protecție pentru registrii sistemului de operare prin aplicarea de politici ce restricționează efectuarea de modificări. De asemenea, trebuie să poată scana registrii de programe malițioase instalate;
56. Sa poată detecta viruși pe email pentru clienții de mail Microsoft Outlook;
57. Sa poată detecta codul malițios din fișierele transferate prin software de genul Instant Messaging;
58. Sa ofere mecanisme de protecție ce nu permit utilizatorului sau aplicațiilor malițioase sa intervină asupra fișierelor/proceselor/cheilor de registrii ale acesteia;
59. Sa blocheze descărcările de fișiere malițioase de pe paginile web;
60. Sa genereze rapoarte cu privire la site-urile pe care utilizatorii încercă să le acceseze;
- Vizibilitatea si managementul traficului web prin prezentarea rapoartelor predefinite care sa conțină cel puțin:
- Top 100 site-uri blocate
- Top Sites Grouped by Content;
- Vîșit Log;
- Download log;

61. Protecția împotrivă:
- Rulării de aplicații din directorul TEMP al sistemului de operare;
- Conexiunilor IRC, TFTP, FTP, SMTP cu excepția aplicațiilor cunoscute si permise;
- Înregistrării automata a programelor ca servicii;
- Modificării/creării de executabile, extensii, procese si setări;

62. Soluția trebuie să poată scana la cerere:
- Memoria sistemelor;
- Procesele ce rulează;
- Partițiile locale;
- Dispozitivele atașate de stocare date;
- Directoare din rețea;
- Registrii

63. Sa permită creare de politici în mod granular de permitere/blocare a dispozitivelor periferice pe baza informațiilor precum:
- ID Producător;
- ID Model Dispozitiv Periferic;
- Tipul de dispozitiv;
- Clasa dispozitivului detectat de sistemul de operare;
- BUS Conectare (USB, S-ATA, ETC.);
- Numele Dispozitivului;
- Tipul sistemului de fișiere (NTFS/FAT/FAT32);
- Numele Volumului/Partiției (In cazul dispozitivelor de stocare date).

64. Sa poată lua următoarele acțiuni la conectarea unui dispozitiv periferic:
- Blocare: Sa nu permită instalarea acestuia;
- Monitorizare: Sa genereze un eveniment ce conține detalii despre dispozitiv;
- Forțare mod utilizare ReadOnly: In cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele;

65. Sa alerteze administratorul atunci când sunt copiate informații pe dispozitive externe de stocare date;
66. Sa ofere posibilitatea de creare a unei reguli de shadowing (duplicare) a fișierelor copiate pe dispozitive externe atunci când anumite criterii sunt îndeplinite (Ex: Un anumit utilizator, grup de utilizatori, tipul fișierului, extensia fișierului). Duplicatul fișierului trebuie sa poată fi accesat numai de cei ce au acest drept in consola de administrare;

Lotul 2. Soluție software pentru protecția împotriva scurgerii de informații (DLP – Data Loss Prevention):

Modelul articolului – McAfee Endpoint Threat Protection with 1year of support;
Țara de origine – SUA;
Producătorul – McAfee.

1. Soluția de tip DLP, la nivel de componente endpoint (agent, module), trebuie să poată rula cel puțin pe: Windows 8 si 8.1, 10 , Enterprise si Professional, 32-bit and 64-bit; Windows 7 SP1 sau mai recente Enterprise si Business, 32-bit and 64-bit; Windows Server 2008/2008R2; Windows Server 2012/2012R2; Windows Server 2016; OS X Yosemite; OS X Mavericks; OS X Mountain Lion; OS X El Capitan
2. Soluția suporta următoarele soluții de tip directory: Microsoft AD si Open LDAP;

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

3. Soluția trebuie sa ofere funcționalități de instalare la distanta pentru agenții de monitorizare astfel încât la momentul instalării sau upgrade să nu fie necesară restartarea sistemelor.;
4. Soluția trebuie sa ofere suport pentru mediile virtuale incluzând VDI, aceasta însemnând ca fiecare politica trebuie să activeze și alerteze pe baza de utilizator. Politicile per user trebuie să se aplice pe sesiuni multiple și să ofere un control și o flexibilitate pe shared terminals sau pe VDI;

Politici de Securitate

5. Soluția va putea aplica politici bazate pe conținut confidențial pentru cel puțin 300 de tipuri de fișiere;
6. Soluția trebuie să ofere mecanisme interne de clasificare manuală pentru fișierelor Microsoft Office sau PDF, soluția propusă va folosi un program de ADD-on pentru MS Office si la momentul salvării utilizatorii vor fi direcționați pentru alegerea nivelului de clasificare intern.;
7. Soluția trebuie sa facă clasificarea conținutului chiar daca acesta este arhivat si trebuie să extragă datele din cel puțin 10 nivele de arhivare;
8. Soluția trebuie sa suporte detectarea documentelor înregistrate/amprentate și clasificate.
9. Soluția trebuie să aibă capabilitatea de a proteja datele bazându-se pe punctul lor de origine/creare;
10. Soluția trebuie sa ofere mecanisme interne de TAG-are sau etichetare a fișierelor folosind metoda fields pentru o categorie șire și căutare mai facilă și mai rapidă;
11. Soluția este capabilă să analizeze conținut și sa aplice politici, indiferent de limba utilizată.;
12. Soluția trebuie să fie capabilă să scaneze și să găsească conținut sensibil;
13. Agentul trebuie sa aibă capabilități de analiză de conținut si blocare pentru mediile optice.;
14. Soluția trebuie sa folosească mai puțin de 5% din procesor in cazul utilizării intense și gradul de utilizare medie este maxim 2% în timpul funcționării normale;
15. Soluția trebuie sa poată proteja informația confidențială care poate fi:
scrisa pe USB/optice;
trimisa pe mail
uploadată pe web
copiată cu ajutorul clipboardului
printata în fișier sau pe imprimantă
scrisă pe un share în rețea
folosită în aplicațiile network – based
aplicații cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive)
16. Soluția trebuie sa poată fi integrate cu o soluție care sa ofere vizibilitate in timp real a amenințărilor pentru prevenirea pierderilor de date;
17. Soluția trebuie sa ofere protecție la nivel de „Clip board" atât pentru copy sau paste cît și pentru screen capture;
18. Soluția trebuie sa permită crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play;
19. Soluția trebuie să ofere același nivel de protecție și în Windows SafeMode;
20. Soluția trebuie sa fie capabilă să facă analiza de conținut local (offline), fără a folosi vreo alta Componența a soluției;
21. Soluția permite auditarea functionalității agentului de endpoint;
22. Soluția trebuie sa permită dezinstalarea agentului in mod centralizat sau in urma unui mecanism de tipul challenge/response;
23. Soluția trebuie sa aibă un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme;
24. Soluția pentru endpoint-uri are capabilitati de clasificare diverse ce nu depind de limbajul folosit: analiza pe termeni/cuvinte cheie, regex-uri si scor de risc, etc;
25. Agentul de endpoint trebuie sa fie compatibil, determinat prin testari, cu solutii de antivirus, firewall, criptare backup si antispyware third-party (de ex: Kaspersky, McAfee, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware);
26. Agentul de endpoint trebuie sa permită aplicarea politicilor folosind conținut înregistrat/ amprentat;
27. Soluția trebuie sa permită realizarea unui proces de justificare, in cazul in care utilizatorul transmite conținut confidențial;

28. Opțiune de justificare a activității folosita de end-user in cadrul procesului de justificare, trebuie sa poată fi validabila sau administrabila;
29. Soluția trebuie sa fie capabilă sa blocheze dispozitivele mobile sau sa permită doar accessul de tip read-only.
30. Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca și criteriu cuvinte-cheie.
31. Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca si criteriu expresii regulate.
32. Soluția trebuie sa poată realiza reguli de protecție care sa aibă ca și criteriu amprenta (hash-uri);
33. Construcția regulilor trebuie sa includă suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

34. Soluția trebuie sa fie capabilă sa aplice următoarele acțiuni: blocare, monitorizare, notificare utilizator, menținere evidenta, criptare sau aplicarea de etichete;
35. Soluția trebuie sa aibă capabilitatea de a se integra cu soft de criptare 3rd party sau al aceluiași producător, pentru a realiza aplicarea politicilor de criptare în funcție de conținut;
36. Regulile de protecție de email la nivel de endpoint, trebuie sa permită bypass-ul, folosind un șir de caractere configurabil in subiectul mesajului, mutând detecția la nivelul gateway-ului de email;
37. Soluția trebuie sa aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true file type si nu doar pe extensia fișierelor;
38. Soluția trebuie sa aibă abilitatea de a face discovery local. De asemenea ea trebuie sa poată conține și o Opțiune de remediere;
39. Soluția trebuie sa fie capabilă sa aplice regulile de protecție atât la nivel de grupuri /useri definiți în Active Directory cât și pentru userii locali ai sistemelor;
40. Soluția trebuie sa fie capabilă sa aplice regulile de control al perifericelor chiar si atunci când nu este conectat la rețeaua instituției, cu posibilitatea de a avea politici diferite in funcție de conectivitatea la rețeaua instituției;
41. Soluția are abilitatea de a face discovery in interiorul bazelor de e-mail stocate pe endpoint.;
42. Soluția trebuie sa permită customizarea notificărilor emise in timpul funcționării si a ferestrei in care sunt scrise aceste notificări;
43. Soluția trebuie sa fie capabilă sa identifice nivelul de clasificare a documentelor din marcajele vizuale si sa aplice regulile de protecție pe aceste documente;
44. Soluția trebuie sa fie capabilă sa protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale;
45. Soluția trebuie sa se integreze nativ cu un produs de clasificarea datelor;
46. Soluția trebuie sa poată aplica etichete fișierelor în funcție de originea lor, informația fiind stocata securizat in Alternate Data Stream pentru a nu putea fi alterata de utilizator;
47. Soluția trebuie sa fie capabilă sa citească informațiile de tip META stocate în fișierele Office;
48. Soluția trebuie sa ofere utilizatorilor posibilitatea de clasificare manuala a documentului la momentul salvării documentelor MS Office;
49. Soluția trebuie sa ofere utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimiterii unui email folosind clientul Outlook office;
50. Soluția trebuie sa ofere politici de securitate out-of-box care pot fi constumizate de către utilizator;
51. Soluția trebuie sa ofere posibilitatea clasificării in timp real pentru a minimiza false pozitive.;
52. Soluția trebuie sa permită protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea.

Consola de administrare

53. Consola de administrare trebuie sa se poată instala pe unul din următoarele sisteme de operare pe 64 de biți:
Microsoft Windows Sever 2016
Microsoft Windows Sever 2012 Release 2 (R2)
Microsoft Windows Server 2012
Windows Server 2008 SP2 Standard, Enterprise, Datacenter
Windows Server 2008 R2 Standard, Enterprise, Datacenter
54. Consola permite pe lângă distribuirea componentelor native si împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru;
55. Consola permite atribuirea automata a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare);
56. Sincronizarea dintre server si client trebuie sa se facă dinspre client către server.
57. Consola de administrare trebuie să se poată integra cu Active Directory.
58. Consola de administrare trebuie sa poată fi instalată intr-un mediu virtual.
59. Consola trebuie sa poată fi instalată în mediu Microsoft Cluster.
60. Consola de administrare trebuie să folosească Microsoft SQL.
61. Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet.

62. Comunicarea dintre componentele soluției și serverul de administrare trebuie să se facă prin intermediul unui singur agent.
63. Soluția trebuie sa permită filtrarea evenimentelor ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile.
64. Soluția trebuie sa permită configurare unui mesaj de login.
65. Soluția poate folosi un proxy pentru contactarea serverului de actualizare al producătorului.
66. Accesul în consola de administrare poate fi făcut pe baza credentialelor din Active Directory.
67. Accesul in consola de management poate fi făcut pe baza certificatelor x509.

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

68. Consola de administrare trebuie sa permită creare de roluri in mod granular pentru cei ce o administrează.
69. Acțiunile utilizatorilor în consola trebuiesc audiate.
70. Consola trebuie sa permită construirea unei liste de contacte in vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail).
71. Canalul de comunicație dintre serverul de administrare și componentele distribuite pe calculatoare trebuie să fie criptat.
72. Componența ce asigură canalul de comunicație dintre server și stații de lucru trebuie sa fie validată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.)
73. Canalul de comunicație dintre consola si cei ce o accesează trebuie să fie criptat.
74. Consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod Web securizat utilizând un browser standard (Internet Explorer, Chrome, Firefox), fără necesitatea instalării de software adițional.
75. Pentru interfața Web a consolei trebuie sa fie posibil importul unui certificat SSL generat de o autoritate locală, înlocuind astfel pe cel auto-generat.
76. Intervalul de sincronizare între server și componente poate fi modificat.
77. Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat.
78. Consola trebuie sa poată detecta prezenta pe rețea a sistemelor noi apărute prin intermediul unor senzori.
79. Consola trebuie să folosească un propriu index pentru a identifica si actualiza datele despre sistemele care își schimba proprietăți precum nume,ip si configurație hardware;
80. Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor si de transmiterea de notificări prin mesagerie electronica.
81. Consola trebuie să prezinte cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare si adresa IP.
82. Consola trebuie sa se integreze cu sisteme de ticketing externe precum BMC Remedy si HP OpenView.
83. Serverul de administrare trebuie sa fie capabil sa declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (Ex: Generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea);
84. Consola trebuie sa permite aplicarea de politici diferite pentru sisteme pe:
Sisteme individuale
Grupuri de sisteme
Sisteme din AD
85. Consola trebuie să știe sa lanseze automat aplicații externe si sa injecteze parametrii din evenimente.
86. Consola permite accesarea logului componentei de sincronizare de pe sisteme in timp real prin intermediul unui serviciu web.
87. Consola trebuie sa permită vizualizarea incidentelor de securitate si crearea de cazuri
88. Evidentele din incidentele de securitate trebuie stocate criptat pe serverul unde rulează consola de management;
89. Consola trebuie sa permită integrarea si altor aplicații/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) intr-o consola unica pentru a unifica administrarea acestora.

Raportare:

90. Consola de administrare poate asigură generarea de rapoarte despre nodurile administrate si despre evenimentele generate de ele.
91. Consola trebuie sa permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.
92. Rapoartele pot fi generate sub forma de tabel, pie chart, buble chart, lista, sumar, sau grafic istoric.
93. Rapoartele pot fi exportate in format pdf, csv, html.
94. Rapoartele pot fi personalizate cu logo-ul instituției
95. Rapoartele pot fi salvate ca fișiere sau trimise prin e-mail.
96. Rapoartele pot fi exportate intr-un format arhivat pentru conservare de lățime de banda si expediate automat pe e-mail unor destinații presetate.
97. Consola permite evaluarea evenimentelor primite de la stațiile de lucru si filtrarea lor pentru o mai buna identificare a informațiilor relevante;
98. Se pot genera rapoarte utilizând:

Logul de audit administrative
Detalii despre sistemele administrate (Detalii de configurare, hardware, utilizator)
Evenimente de la sisteme
Informații despre politicile si sarcinile aplicate sistemelor
Informații furnizate de senzori

Serviciu Instalare, configurare și training

99. Ofertantul selectat va efectua pregătirea mediului de instalare pentru Soluția propusă, după care va asigură implementarea inițială a soluției aplicative în mediul de producție și mediul de testare al (clientului).

Anexa nr. 1(continuare)
la contractul nr. 54 LP
din 16 octombrie 2018

100. Ofertantul selectat va pregăti un plan de acțiuni și implementare care urmează a fi aprobat, în baza căruia se va realiza implementarea.

101. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială, (Furnizorul) înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție.

102. În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările / customizările agreate darea în exploatare a soluției.

103. Ofertantul va asigură integrarea soluției cu cel puțin următoarele aplicații terțe: Integrarea cu Active Directory – pentru a asigură autentificarea utilizatorilor în cadrul soluției prin AD; Integrarea cu platforma mobila (telefoane, tablete) – pentru securizarea perimetrului mobile. Integrarea cu alte platforme pe care se va instala produsul.

104. La sfîrșitul etapei, Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare.

105. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post-implementare si suport. Perioada de garanție post-implementare si suport va fi de 1 an calendaristic de la data activării acestei opțiuni. Serviciile de garanție post-implementare si suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor.

106. Serviciile de garanție post-implementare si suport, vor include următoarele componente:
Gestionarea incidentelor de securitate apărute pe perioada suportului activ;
Solicitărilor de schimbare a politicilor de securitate
Solicitări de analiză și corecție a politicilor de securitate.

Lotul 5. Server

Modelul articolului – Server MaguayMaguay eXpertServer;
Țara de origine – România;
Producătorul – Maguay.

1. Format Rackmount - 2U, (H x W x D): 660 x 430 x 88 mm
2. Supported CPUS - Dual-CPU support: echivalent Intel Xeon E5-26xx , max. 135W, 2*QPI link, VTd
3. CPU - 1x Processor echivalent - Intel® Xeon® Processor E5-2640v2, Eight Core
4. Chipset - echivalent Intel C600-A
5. RAM- 32 GB 1600 MHz REG DDR3, Quad-channel per CPU; maxim 512GB DDR3 REG ECC, minim 16 slot-uri
6. HDDs - 2*300 GB SAS 15k + 2*1TB SATA Enterprise
7. Bays - 8* hot-swap 3.5
8. RAID - RAID 0,1, 10
9. Slots -5 x PCIe 2.0 x8, 1x PCIe 3.0 x16
10. Networking - 3 Gigabit Ethernet
11. Ports - 6*USB 2 & 1 x serial, 1 x VGA, 4 x RJ45
12. VGA - Integrated 2D Video Controller 16MB DDR3
13. Power Supply - 500W high efficiency PSU Active Controls - Front Control panel with power and reset buttons, indicator LEDs
14. Management - IPMI 2.0, Intel System Management Software, Intel Remote Management Module
15. Dotare/compatibil cu Sistem de Operare: Windows Server 2016 for motherboard with 2 CPU,
16. Sitem Operare Support: - Windows Server, Linux (Red Hat Enterprise Linux, SuSE Linux Enterprise Server), Vmware Ready
17. Se accepta produse Refurbished.

Garanție: 24 luni

„Vânzătorul”:

Viorica ODOBESCU

L.Ș.

„Cumpărătorul”:

Serghei DEMCENCO

L.Ș.

Anexa nr. 2
la contractul nr. 54 LP
din 16 octombrie 2018

№		*Denumirea bunului*		
		Licenţă Antivirus (echivalent McAfee Endpoint Protection)	**Soluție software pentru protecția împotriva scurgerii de informații (DLP – Data Loss Prevention)**	**Server**
	Cantitate (metri/bucăți)	**200 buc.**	**50 buc.**	**1 buc.**
	Inclusiv pe luni			
	Ianuarie			
	Februarie			
	Martie			
	Aprilie			
	Mai			
	Iunie			
	Iulie			
	August			
	Septembrie			
	Octombrie	**200 buc.**	**50 buc.**	**1 buc.**
	Noiembrie			
	Decembrie			
	Suma alocațiilor (lei)			
	Ianuarie			
	Februarie			
	Martie			
	Aprilie			
	Mai			
	Iunie			
	Iulie			
	August			
	Septembrie			
	Octombrie			
	Noiembrie			
	Decembrie			
	Art. clasif. bugetare			
	Alineatul			

„Vânzătorul”:

Viorica ODOBESCU

L.Ș.

„Cumpărătorul”

Serghei DEMCENCO

L.Ș.