ANUNŢ DE PARTICIPARE

privind achiziţionarea Pachete software şi sisteme informatice, Pachete software antivirus conform necesităţilor Armatei Naţionale.

prin procedura de achiziţie Licitaţie deschisă

1. Denumirea autorităţii contractante: Agenţia asigurare resurse şi administrare patrimoniu a Ministerului Apărării

2. IDNO: 1006601001229

3. Adresa: mun. Chişinău, şos. Hînceşti 84

4. Numărul de telefon/fax: 022-25-22-09 25-23-57 25-23-00 / 022 25 20 49

5. Adresa de e-mail şi de internet a autorităţii contractante: vitalie.rohac@army.md

6. Adresa de e-mail sau de internet de la care se va putea obţine accesul la documentaţia de atribuire: documentaţia de atribuire este anexată în cadrul procedurii conform ***SIA "RSAP"***

7. Tipul autorităţii contractante şi obiectul principal de activitate (dacă este cazul menţiunea că autoritatea contractantă este o autoritate centrală de achiziţie sau că achiziţia implică o altă formă de achiziţie comună): Autoritate centrală de achiziţie a Ministerului Apărării.

8. Cumpărătorul invită operatorii economici interesaţi care îi pot satisface necesităţile să participe la procedura de achiziţie privind livrarea/prestarea/executarea următoarelor bunuri /servicii/lucrări:

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	U/M	Canti-tatea	Specificarea tehnică deplină solicitată. Standarde de referinţă	Valoarea estimată fără TVA
1.	48000000-8	Pachete software şi sisteme informatice	buc	1	OS Licenses: Microsoft Windows Server 2019 +50 call-uri. WinSvrSTDCore ENG LicSAPk OLP 16Lic A Gov CoreLic; WinSvrCAL 2019 ENG OLP A Gov DvcCAL - licenţe permanente pentru 50 PC-uri. ***Cerinţe minime de calificare a ofertanţilor:*** *1.1. Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanţă, inclusiv suport local din partea partenerului.* *1.2. Prezentare a minim 2 certificate tehnice al ofertantului;* *1.3. Lucrările de instalare, configurare, punerea în funcţiune a soluţiei trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.* *1.4. Ofertantul trebuie sa fie certificat ISO 9001 şi 27001. Prezentarea documentelor justificate este obligatorie.* *1.5. Prezentarea autorizării de la Producător (MAF);* *1.6. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova;* *Termen livrare: pînă la 30 zile de la data intrării în vigoare a contractului, care include şi timpul lucrărilor de instalare, configurare şi punerea în funcţiune a soluţiei.*	775900,00
2.	48000000-8	Pachete software antivirus	buc	1	Soft Antivirus (Produsul Antivirus va acoperi următoarea infrastructură: PC-uri fizice şi virtualizate, servere fizice şi virtualizate, căsuţe poştale pe Exchange şi mobile/tablete (Android & IOS), 760 licenţe, până la 1140 căsuţe poştale pe Exchange;	57500,00

					Patch Management pentru 760 dispozitive, 36 luni; Full Disk Encryption pentru 70 dispozitive, 36 luni) **CARACTERISTICI GENERALE ALE PRODUSULUI** Produsul este o platformă integrată pentru managementul securităţii, gândită ca o soluţie modulară de protecţie şi securitate pentru 735 calculatoare, **5** servere fizice, 10 servere virtuale, 10 dispozitive mobile şi peste 1000 căsuţe poştale pentru o perioadă de 36 luni. Produsul conţine următoarele module: **A.** O consola de management care asigura funcţionalităţi de administrare dintr-o singură consolă; **B.** Protecţie staţii şi servere fizice/virtuale: - *Windows 10,8.1,7, Vista (SP1), XP (SP3), Mac OS X 10.12.x, 10.11.x, 10.10.x, 10.9.x, 10.8.x .* - *Windows Server 2003/2008/2008 R2/2012/2012 R2/2016/2019.* - *Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Oracle Linux 6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual, Debian 5.0 sau mai recent.* **C.** Protecţie şi securitate pentru telefoanele mobile de tip smartphone cu *sistem de operare iOS şi Android;* **D.** Protecţie şi securitate pentru serverele *email* Microsoft *Exchange*. **E.** Integrare SIEM. **A.** CONSOLA DE MANAGEMENT **1. Instalare şi configurare:** 1.1. Pachetul de instalare va fi livrat ca o maşină virtuală preinstalată care conţine toate rolurile şi serviciile necesare. Consola nu va necesita o licenţa suplimentară pentru sistemul de operare. Imaginea de tip template va putea fi importată în unul din următoarele sisteme de operare: 1.1.1. Vmware vSphere 1.1.2. Microsoft Hyper-V 1.1.3. Red Hat Enterprise Virtualization 1.1.4. KVM 1.1.5. Oracle VM etc. 1.2. Consola de management se livrează cu o baza de date inclusă care este de tip non-relaţională, pentru o funcţionare cât mai rapidă, fără a fi nevoie de licenţe adiţionale. 1.3. Soluţia va fi scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe maşini virtuale sau pe aceeaşi maşină virtuală. 1.4. Rolurile principale trebuie să fie cel puţin similare cu: Serverul cu bază de date, Serverul de comunicaţie, Serverul de actualizare, Serverul de Web. 1.5. Să asigure posibilitatea de a instala serviciile de scanare centralizată pentru mediile virtuale Vmware şi Citrix prin task din consola de management. 1.6. Soluţia va include adiţional şi un modul de balansare (loadbalancer) pentru cazurile în care mai multe maşini virtuale ale componentei de management sunt instalate cu acelaşi rol (pentru LoadBalancing şi performanţă/redundanţă). 1.7. Soluţia va include un mecanism de configurare a disponibilităţii pentru Serverul cu baze de date (clustering pentru redundantă). Astfel, baza de date se	

					va putea instala de mai multe ori, pe mai multe maşini virtuale. 1.8. Să includă posibilitatea de a fi accesată atât de pe staţiile de lucru cât şi de pe dispozitivele mobile (tabletă, smartphone). **2. Cerinţe generale:** 2.1. Interfaţa consolei de management va fi cel puţin în două limbi (engleză şi română). 2.2. Interfaţa clientului de securitate, care se instalează pe staţii şi servere, va avea posibilitatea de a fi instalată cel puţin în două limbi (engleză şi română). 2.3. Manualul de instalare a produsului va fi în limba română şi sau engleză. 2.4. Manualul de administrare a produsului va fi în limba română şi sau engleză. 2.5. Soluţia va include un modul de update server prin care se asigură actualizarea de produs şi a semnăturilor. 2.6. Soluţia va permite activarea/dezactivarea actualizărilor de produs/semnături. 2.7. Soluţia va permite stabilirea actualizării automate a consolei de management prin stabilirea recurentei zilnice, săptămânale sau lunare, dar şi prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, va permite şi trimiterea unei alerte de ne funcţionalitate, cu 30 de minute înainte de actualizare. 2.8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluţia permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: 2.8.1. versiunea consolei de management 2.8.2. data versiunii 2.8.3. funcţii noi şi îmbunătăţiri 2.8.4. probleme rezolvate 2.8.5. probleme cunoscute 2.9. Notificările – prezente în interfaţă, notificările necitite sunt evidenţiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licenţiere, detecţie viruşi, actualizări de produs disponibile. 2.10. Soluţia va permite integrarea cu un server Syslog pentru raportarea evenimentelor anti malware. 2.11. Soluţia va permite instalarea serviciului de SMNP prin care se pot raporta statusul maşinilor din cadrul componentei de management. 2.12. Soluţia va permite crearea unei copii de siguranţă a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în reţea. **3. Panou de monitorizare şi raportare (Dashboard):** 3.1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ţinta raportului, opţiuni specifice pentru orice tip de raport. 3.2. Panoul central conţine rapoarte pentru toate modulele suportate. 3.3. Rapoartele din panoul central de comandă permit: adăugarea altor rapoarte, ştergerea lor şi rearanjarea. **4. Inventarierea reţelei – managementul securităţii:** 4.1. Soluţia se va integra cu domenii Active	

					Directory multiple, VmwarevCenter, Citrix Xen şi importa inventarul acestor platforme. 4.2. Pentru integrarea cu Active Directory, se va putea defini şi intervalul (în ore) de sincronizare şi forţa sincronizarea. 4.3. Se va permite descoperirea maşinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 4.4. Se va permite descoperirea staţiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 4.5. Soluţia va oferi opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare şi adresa IP. 4.6. Soluţia va permite instalarea la distanţă sau manual a clienţilor anti malware pe maşini fizice/virtuale. 4.7. Soluţia va permite selectarea modulelor componente, atunci când se creează pachetul clientului care se instalează pe maşinile fizice/virtuale. 4.8. Soluţia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanţă pentru clientul anti malware. 4.9. Soluţia va oferi posibilitatea de repornire a maşinilor fizice de la distanţă. 4.10. Soluţia va oferi informaţii detaliate despre fiecare task şi va afişa daca task-ul s-a finalizat sau nu cu succes. 4.11. Soluţia va permite configurarea centralizată a clienţilor anti malware prin intermediul politicilor. 4.12. Se vor oferi în consola de management informaţii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 4.13. Soluţia permite descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea, prin rularea unui task din consola de administrare. Astfel, administratorul va putea descărca pachetele pentru protecţia staţiilor şi serverelor pe care rulează SO Windows, Linux şi Mac. **5. Politici:** 5.1. Soluţia va permite configurarea setărilor clientului anti malware prin intermediul unei singure politici ce conţine setări pentru toate modulele. 5.2. Politica va conţine opţiuni specifice de activare/dezactivare şi configurarea funcţionalităţilor precum scanarea anti malware la cerere, firewall, controlul accesului la Internet, controlul aplicaţiilor, scanarea traficului web, controlul dispozitivelor, utilizator cu drepturi privilegiate (poweruser). 5.3. Soluţia va permite aplicarea politicilor pe maşini client, grupuri de maşini, pool-uri de resurse (VMware), domeniu, unităţi organizaţionale sau utilizatori din Active Directory. 5.4. Politica să poată fi schimbată automat în funcţie de: 5.4.1. User-ul logat pe staţie 5.4.2. IP sau clasa de IP al staţiei 5.4.3. Gateway-ul alocat 5.4.4. DNS serverul alocat 5.4.5. Clientul este/nu este în aceeaşi reţea cu infrastructura de management 5.4.6. Tipul reţelei (lan, wireless) **6. Rapoarte:**	

					6.1. Soluţia va permite generarea rapoartelor care prezintă statutul maşinilor clienţilor din punct de vedere al actualizărilor, fişierelor malware detectate, aplicaţiile blocate, site-urilor web blocate. 6.2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management). 6.3. Soluţia va permite vizualizarea rapoartelor curente programate de administrator. 6.4. Soluţia va permite exportarea rapoartelor în format .pdf şi detaliile ca format .csv. 6.5. Soluţia va include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menţinând informaţiile concise şi ordonate corespunzător. 6.6. Interogarea legată de starea terminalului include informaţii precum: 6.6.1.tip maşină 6.6.2.infrastructura reţelei căreia ii aparţine terminalul 6.6.3.datele agentului de securitate 6.6.4.starea modulelor de protecţie 6.6.5.rolurile terminalelor. 6.7. Interogarea legată de evenimente terminal include informaţii precum: 6.7.1.calculatorul ţintă pe care a avut loc evenimentul 6.7.2.tipul starea şi configuraţia agentului de securitate instalat 6.7.3.starea modulelor şi rolurilor de protecţie instalate pe agentul de securitate 6.7.4.denumirea şi alocarea politicii 6.7.5.utilizatorul autentificat în timpul evenimentului 6.7.6.evenimente (site-uri blocate, aplicaţii blocate, detecţiile etc.) 6.8. Interogarea legată de evenimente Exchange include informaţii precum: 6.8.1.Direcţia traficului e-mail 6.8.2.Evenimente de securitate (detectarea programelor de tip malware sau a fişierelor ataşate) 6.8.3.Măsurile implementate în fiecare situaţie (curăţarea, ştergerea, înlocuirea sau punerea în carantină a fişierului, ştergerea sau respingerea e-mail-ului) **7. Carantina:** 7.1. Soluţia va permite restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă. 7.2. Locaţia, fişierele şi administrarea Carantinei trebuie să fie efectuată central din consola de management. 7.3. Permite descărcarea fişierelor din carantină doar pentru maşinile virtuale protejate prin modulul mediilor virtuale integrat cu Vmware vShield. **8. Utilizatori:** 8.1. Administrarea se va putea face pe bază de roluri. 8.2. Roluri multiple predefinite: Administrator companie, Administrator reţea, Reporter sau rol personalizat. 8.3. Administrator companie: administrează arhitectura consolei de management; 8.4. Administrator reţea: administrează serviciile de securitate; 8.5. Reporter: monitorizează şi generează rapoarte. 8.6. Utilizatorii pot fi importaţi din Microsoft Active Directory sau creaţi în consola de management.	

					8.7. Se va permite configurarea detaliată a drepturilor administrative, permiţând selectarea serviciilor şi obiectelor pentru care un utilizator poate face modificări. 8.8. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp. **9. Log-uri:** 9.1. Înregistrarea acţiunilor utilizatorilor. 9.2. Se vor oferi informaţii detaliate pentru fiecare acţiune a unui utilizator. 9.3. Se va permite filtrarea acţiunilor utilizatorului după numele utilizatorului şi după acţiune. **10. Actualizare:** 10.1. Se permite definirea de locaţii de actualizare multiple. 10.2. Se permite activarea/dezactivarea actualizărilor de produs şi semnături. 10.3. Se permite actualizarea produsului într-o reţea fără acces la Internet. 10.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus 10.5. Soluţia va putea fi instalată pe un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenţia administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecţia staţiilor şi serverelor pe care rulează sistemul de operare Windows sau Linux sau poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare VMwaresauHyper-V. 10.6. În cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecţia staţiilor şi serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric: 10.6.1. versiunea pachetului 10.6.2. data versiunii 10.6.3. funcţii noi şi îmbunătăţiri 10.6.4. probleme rezolvate 10.6.5. probleme cunoscute 10.7. Soluţia permite testarea noilor versiuni de pachete de instalare ale clientului anti malware, înainte de a fi instalate pe toate staţiile şi serverele din reţea, evitând posibile probleme ce pot afecta serverele sau staţiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: 10.8. Ciclu rapid, gândit pentru un mediu de test în cadrul reţelei 10.9. Ciclu lent, gândit pentru restul reţelei (producţie, servere critice etc.) 10.10. Soluţia permite stabilirea zonelor de test şi critice din cadrul reţelei prin intermediul politicilor din consola de management. **B.** PROTECŢIE STAŢII şi SERVERE FIZICE/VIRTUALE **1. Caracteristici generale minimale şi eliminatorii:** 1.1. Pentru reducerea la minim a consumului de resurse, soluţia anti malware trebuie să permită instalarea personalizată a modulelor deţinute (de exemplu, să permită instalarea soluţiei anti malware fără modulul de control al accesului web, modul de	

					control al dispozitivelor sau modulul firewall). 1.2. Pentru o mai buna protecţie a staţiilor şi serverelor, soluţia include un vaccin anti-ransomware. Acest vaccin asigură protecţia împotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea staţiilor şi serverelor, chiar daca sunt infectate şi prin blocarea procesului de criptare. 1.3. Vaccinul anti-ransomware primeşte actualizări de la producător, odată cu actualizarea semnăturilor produsului Anti malware. 1.4. Pentru o mai buna protecţie a staţiilor şi serverelor, soluţia include protecţie împotriva atacurilor zero-day de tip exploit (atacuri direcţionate). 1.5. Includă module avansate de securitate, proiectate special pentru a detecta atacuri avansate şi activităţi suspecte în faza pre-execuţie, pentru protecţie împotriva: atacurilor direcţionate (Targeted Attack - APT), fişierelor suspecte şi traficului la nivel de reţea suspect, exploit-urilor, ransomware şi grayware cu posibilitatea de stabilire a nivelului de protecţie dorit: permisiv, normal, agresiv cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare. 1.6. Includă un sandbox în cloud-ul producătorului, ce va putea trimite manual sau automat fişiere, unde vor putea fi „detonate” pentru o analiză în profunzime. 1.7. Includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acţiuni de remediere: implicită şi de siguranţă. Pentru acţiunea implicită: doar raportare, dezinfecţie, ştergere şi transmitere în carantină. Pentru acţiunea de siguranţa: ştergere sau permutare în carantină. 1.8. Modulul de Sandbox va include si posibilitatea de trimitere manuală a fişierelor in Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fişier ca fiind maliţios, îl poate trimite manual in Sandbox pentru a fi „detonat” şi a afla verdictul. Va putea trimite mai multe fişiere de odată, cu posibilitate de a specifica dacă vor fi „detonate” individual sau toate în acelaşi timp. Acced modul va poatea suporta „detonarea” următoarelor tipuri de fişiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Aceste fişiere menţionate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. **2. Cerinţe de sistem:** 2.1. Sisteme de operare pentru staţii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3) sau mai recent. 2.2. Sisteme de operare embedded: Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POS Ready 7, Windows Embedded Enterprise 7, Windows Embedded POS Ready 2009, Windows Embedded Standard 2009, Windows XP	

					Embedded with Service Pack 2, Windows XP Tablet PC Edition. 2.3. Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server sau mai recent. 2.4. Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual,Debian 5.0 sau mai recent. **3. Administrare şi instalare remote:** 3.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user. 3.2. Instalarea se va putea face în mai multe moduri: 3.2.1. prin descărcarea directă a pachetului pe staţia pe care se va face instalarea; 3.2.2. prin instalarea la distanţă, direct din consola de management. 3.2.3. trimiterea pe email (oricare adrese) a pachetului de instalare pentru Windows, Linux, Mac. 3.2.4. Instalarea clienţilor la distanţă în alte locaţii decât cele în care este instalată consola de management se va face prin intermediul unui alt client antivirus existent în locaţiile respective pentru a minimiza traficul în WAN. 3.2.5. Consola trebuie să includă o secţiune, „Audit”, unde se vor păstra toate acţiunile întreprinse de administratori şi utilizatori ai consolei, cu informaţii detaliate: logare, editare, creare, delogare, permutare etc. 3.2.6. Din consola se va putea trimite o singură politică pentru configurarea integrală a clientului de pe staţii/servere. 3.2.7. Consola va include o secţiunea, unde se vor menţiona toate acţiunile întreprinse fie de administratori, fie de reporteri, cu informaţii detaliate: logare, editare, creare, delogare, mutare etc. 3.2.8. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biţi, cât şi pentru cele pe 64 de biţi. 3.2.9. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru staţii (fizice si/sau virtuale), servere (fizice şi/sau virtuale), Exchange. 3.2.10. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. 3.2.11. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta staţiile/serverele din reţea pentru cele care nu sunt integrate în domeniu. 3.2.12. Permite selectarea clientului care va efectua descoperirea staţiilor din reţea, altele decât cele integrate în domeniu. **4. Caracteristici şi funcţionalităţi principale ale modulului anti malware:** 4.1. Soluţia permite administratorului să stabilească acţiunea luată de produsul Anti malware la detectarea unei ameninţări noi. Astfel, administratorul va putea alege intre următoarele acţiuni:	

					4.1.1. Acţiune implicită pentru fişiere infectate: 4.1.1.1.interzice accesul 4.1.1.2.dezinfectează 4.1.1.3.ştergere 4.1.1.4.mută fişierele în carantină 4.1.1.5.nici o acţiune 4.1.2. Acţiune alternativă pentru fişierele infectate: 4.1.2.1.interzice accesul 4.1.2.2.dezinfectează 4.1.2.3.ştergere 4.1.2.4.mută fişierele în carantină 4.1.3. Acţiune implicită pentru fişierele suspecte: 4.1.3.1.interzice accesul 4.1.3.2.ştergere 4.1.3.3.mută fişierele în carantină 4.1.3.4.nici o acţiune 4.1.4. Acţiune alternativa pentru fişierele suspecte: 4.1.4.1.interzice accesul 4.1.4.2.ştergere 4.1.4.3.mută fişierele în carantină 4.2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fişiere mai mari de « x » MB, mărimea fişierelor putând fi definită de administratorul soluţiei, 4.3. Definirea nivelelor de profunzime pentru scanarea în arhive. 4.4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicaţii cu potenţial periculos, protejând sistemul de aplicaţii maliţioase necunoscute prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 4.5. Scanarea oricărui suport de stocare a informaţiei (CD-uri, harduri externe, unităţi partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unităţi care au informaţii stocate mai mult de « x » MB. 4.6. Scanarea automată a emailurilor la nivelul staţiei de lucru pentru POP3/SMTP. 4.7. Definirea până la 16 nivele de profunzime pentru scanarea în arhive. 4.8. Configurarea căilor ce urmează a fi scanate la cerere. 4.9. Clienţii anti malware pentru staţiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real şi la cerere a anumitor directoare, discuri, fişiere, extensii sau procese. 4.10. Cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware. 4.11. Posibilitatea de a configura scanările programate să se execute cu prioritate redusă 4.12. Produsul anti malware poate fi configurat să folosească scanarea în cloud, şi parţial scanarea locala. Pentru staţiile ce nu au suficiente resurse hardware, scanarea se poate face cu o maşina de scanare instalată în reţea. 4.13. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: 4.13.1. Configurarea scanării în cloud sau pe maşina de scanare instalată în reţea şi parţial scanarea locală pentru staţiile ce nu au suficiente resurse hardware 4.13.2. Administratorului să personalizeze şi motoarele de scanare, având posibilitatea de a alege	

					între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid. 4.13.3. Setarea tipurilor de detecţie: bazate pe semnături, bazate de comportamentul fişierelor şi bazate pe monitorizarea proceselor. 4.13.4. Scanarea paginilor web. 4.13.5. Setarea unei parole pentru protecţie la dezinstalare. 4.13.6. Modul de antiphishing. 4.13.7. Protecţie în timp real pe maşinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 4.13.8. Instalarea clientului pe maşinile virtuale parte a unui pool doar pe maşina de tip template, după care se recompune pool-ul de maşini virtuale. **5. Firewall:** 5.1. Posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate. 5.2. Modulul poate fi instalat/dezinstalat în funcţie de preferinţa administratorului. 5.3. Posibilitatea de a defini reţele de încredere pentru maşina destinaţie. **6. Carantina:** 6.1. Produsul anti malware să permită trimiterea automata a fişierelor din carantină în locaţia originală sau într-o cale configurabilă. 6.2. Trimiterea conţinutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 6.3. Produsul anti malware să permită ştergerea automata a fişierelor din carantină mai vechi de o anumita perioada, pentru a nu încărca inutil spaţiul de stocare. 6.4. Posibilitatea de a restaura un fişier din carantină în locaţia lui originală. 6.5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături. 6.6. Locaţia, fişierele şi administrarea Carantinei trebuie să fie efectuată central din consola de management. **7. Protecţia datelor:** 7.1. Produsul permite blocarea datelor confidenţiale (pin-ul cardului, cont bancar etc.) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **8. Controlul conţinutului:** 8.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularităţi: 8.1.1. Permite blocarea accesului la Internet pentru anumite maşini client sau grupuri de maşini. 8.1.2. Permite blocarea accesului la Internet pe intervale orare. 8.1.3. Permite blocarea paginilor de Internet care conţin anumite cuvinte cheie. 8.1.4. Permite controlul accesului numai la anumite pagini de internet specificate de administrator; 8.1.5. Permite blocarea accesului la anumite aplicaţii definite de administrator; 8.1.6. Permite blocarea descărcării unor anumite	

					tipuri de extensii de fişiere, definite de administrator (ex: .exe, .zip, .rar, .mp3 etc.) 8.1.7. Permite restricţionarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenţă, pornografie etc.). **9. Controlul aplicaţiilor:** 9.1. Soluţia va include o secţiune în consola de administrare unde se vor regăsi toate aplicaţiile descoperite în reţea, grupate după: nume, versiune, descoperit la, găsit pe. 9.2. Soluţia va include o secţiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în reţea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. 9.3. Soluţia include opţiunea de a permite sau a bloca rularea anumitor aplicaţii sau procese definite de administrator (inclusiv sub procese) după: 9.3.1. Cale fişier: local, CD-ROM, portabil sau reţea; 9.3.2. Hash; 9.3.3. Certificat. **10. Controlul dispozitivelor:** 10.1. Modulul poate fi instalat/dezinstalat în funcţie de preferinţa administratorului. 10.2. Modulul va permite controlul următoarelor tipuri de dispozitive: 10.2.1. Bluetooth Devices 10.2.2. CDROM Devices 10.2.3. Floppy Disk Drives 10.2.4. Security Policies 153 10.2.5. IEEE1394, IEEE1284.4 10.2.6. ImagingDevices 10.2.7. Modems 10.2.8. Tape Drives 10.2.9. Windows Portable (including USB devices and ports) 10.2.10. COM/LPT Ports 10.2.11. SCSI Raid 10.2.12. Printers 10.2.13. NetworkAdapters 10.2.14. Wireless NetworkAdapters 10.2.15. InternalandExternalStorage 10.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la maşina client. 10.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. **11. Power User:** 11.1. Modulul poate fi instalat/dezinstalat în funcţie de preferinţa administratorului. 11.2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa şi modifica setările clientului anti malware dintr-o consola disponibilă local pe maşina client. 11.3. Administratorul va putea suprascrie din consola setările aplicate de utilizatorii Power User. **12. Actualizare:** 12.1. Posibilitatea efectuării actualizării la nivel de staţie în mod silenţios (fără avertizări). 12.2. Sistem de actualizare în trepte (cascadat)	

					folosind unul sau mai multe servere de actualizare (cascadate). 12.3. Actualizarea pentru locaţiile remote prin intermediul unui client anti malware care are şi rol de server de actualizare. **C.** PROTECŢIE ŞI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE **1. Cerinţe minime de sistem:** 1.1. Produsul trebuie să ofere client de protecţie pentru dispozitive mobile cu platforma Android (de la v. 2.2) şi iOS (de la v 5.) sau mai recente **2. Caracteristici:** 2.1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory. 2.2. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare. 2.3. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR. 2.4. Pachetele de instalare se vor putea descărca de pe Apple App Store şi Google Play. 2.5. Se vor putea întreprinde următoarele acţiuni: 2.5.1. Blocarea dispozitivului; 2.5.2. Deblocarea dispozitivului; 2.5.3. Ştergerea datelor şi revenirea la setările din fabrică; 2.5.4. Localizarea dispozitivului; 2.5.5. Scanarea dispozitivului (doar pentru cele cu sistem de operare Android); 2.5.6. Criptarea memoriei dispozitivului (doar pentru cele cu sistem de operare Android); 2.5.7. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbrokendevices). **3. Setări de securitate:** 3.1. În cazul în care un dispozitiv nu este conform cu setările dorite, se vor putea întreprinde automat acţiunile: 3.1.1. Ignorare; 3.1.2. Blocarea accesului; 3.1.3. Blocarea dispozitivului; 3.1.4. Ştergerea datelor şi revenirea la setările din fabrică; 3.1.5. Ştergerea dispozitivului din consolă. 3.2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parolă va putea fi configurata să conţină: 3.2.1. Parolă simplă sau complexă (în funcţie de cerinţele sistemului de operare); 3.2.2. Numere şi litere; 3.2.3. O lungime minimă definită de administrator; 3.2.4. Un număr minim de caractere speciale, definit de administrator; 3.2.5. Perioada de expirare a parolei. Perioada va putea fi definită de administrator; 3.2.6. Configurarea restricţiei refolosirii parolei; 3.2.7. Numărul de introduceri incorecte a parolei, de către utilizator; 3.2.8. Perioada de autoblocare a dispozitivului după un număr de minute definite de administrator. 3.3. Se vor putea genera mai multe profiluri care vor	

					stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS), dar şi unele legate de accesul la anumite pagini de internet. 3.4. Profilurile de Wi-Fi vor conţine următoarele opţiuni: 3.4.1. Generale – se defineşte SSID precum şi tipul securităţii reţelei; 3.4.2. Setări TCP/IP – atât pentru protocolul IPv4, dar şi pentru IPv6; 3.4.3. Setări de proxy – dezactivat, automat sau configurat manual. 3.5. Profilurile acces pagini de internet pentru sistemul de operare Android vor include opţiuni precum: 3.5.1. Permiterea, blocarea sau programarea pentru anumite zile şi intervale orare a accesului la anumite pagini de internet; 3.5.2. Crearea unor excepţii pentru blocarea sau permiterea accesului către anumite pagini de internet. 3.6. Profilurile acces pagini de internet pentru sistemul de operare iOS vor include opţiuni de activare sau dezactivare a: 3.6.1. Utilizării browser-ului Safari; 3.6.2. Opţiunii de completare automată a informaţiilor; 3.6.3. Alertării utilizatorului în cazul accesării unor pagini frauduloase; 3.6.4. Java script; 3.6.5. Pop-up-urilor; 3.6.6. Cookie-uri. **D.** PROTECŢIE ŞI SECURITATE PENTRU SERVERELE DE MAIL MICROSOFT EXCHANGE 1. Va consta în: 1.1. Produsul va oferi protecţie anti malware, anti spam (inclusiv antiphishing), precum şi filtrare de ataşamente şi conţinut, prin integrarea cu serverul Microsoft Exchange cu posibilitatea de scanare a antivirus la cererea bazelor de date Exchange. 1.2. Produsul va asigura scanarea ataşamentelor şi a conţinutului mesajelor în timp real, fără a afecta vizibil performanţa serverului de mail. 1.3. Actualizarea antivirus trebuie să poată fi făcută automat la un interval de maxim 1 oră, precum şi la cerere. 1.4. Modulul de protecţie antivirus va trebui să includă şi scanare euristica comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate şi analizate aplicaţii cu potenţial periculos, pentru a proteja sistemul de viruşii necunoscuţi prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 1.5. Produsul va oferi opţiuni multiple de acţiune la identificarea unui ataşament virusat (dezinfectare, ştergere, mutare în carantină). 1.6. Produsul va oferi protecţie anti-spyware pentru a preveni furtul de date confidenţiale. 1.7. Produsul va oferi protecţie anti spam, cu o bază de semnături actualizată prin internet. 1.8. Modulul antispam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum şi un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice. 1.9. Produsul va trebui să ofere filtru RBL care să	

					identifice spam-ul prin sincronizarea cu anumite baze de date online care conţin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 1.10. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătăţirea protecţiei împotriva valurilor de spam nou apărute. 1.11. Produsul va oferi posibilitatea de a defini politici de filtrare anti malware, anti spam, a conţinutului sau ataşamentelor pentru diferite grupuri sau utilizatori. 1.12. Actualizarea produsului va fi configurabilă şi se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul reţelei de pe un server de actualizare propriu. 1.13. Produsul va trebui să ofere statistici atât referitoare la scanarea antivirus cat şi la scanarea anti spam. 1.14. Produsul se va integra în cadrul consolei de management unitar al soluţiei antivirus. Pentru uşurinţa accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web. **E.** CERINŢE FAŢĂ DE PATCH MANAGEMENT: 1. Soluţia pentru managementul actualizării aplicaţiilor exploatate* pentru 200 staţii de lucru: Bitdefender GravityZone Patch Managemnt sau echivalentul. Soluţia trebuie să acopere următoarele funcţionalităţi minime: 1.1. Integrarea clientului de patch management cu clientul Antivirus, ca un modul separat. 1.2. Administrarea produsului trebuie să fie realizată din aceeaşi consolă de management ca şi soluţia de protecţie antivirus pentru mediul fizic (staţii şi servere), mediul virtual (VDI-uri şi servere virtuale), căsuţe de email Exchange şi dispozitive mobile (Android si iOS). 1.3. Abilitatea de a funcţiona în mod automat cu următoarele presetări: 1.3.1. Programarea evaluării pentru patch-ul lipsă. 1.3.2. Programarea instalării automate, în baza categoriei de patch-uri (securitate / non-securitate). 1.3.3. Posibilitatea de a amâna repornirea, dacă instalarea patch-ului o cere. 1.4. Opţiunea de a iniţia scanarea, descoperirea şi instalarea de patch-uri la cerere. 1.5. Posibilitatea de a vedea toate patch-urile care lipsesc din infrastructură şi agregarea lor într-un inventar de patch-uri. 1.6. Vizibilitatea de patch-uri instalate şi a celor lipsă pe staţiile de lucru. 1.7. Informaţii despre patch-uri instalate şi motivul sau cauza instalării nereuşite. 1.8. Posibilităţi de a instala rapid patch-uri lipsă. 1.9. Posibilitatea de a stopa instalarea unuia sau a mai multor patch-uri/update-uri. 1.10. Notificarea periodică privind statutul infrastructurii, patch-uri instalate, patch-uri lipsă 1.11. Stocarea locală a patch-urilor primite. **-(7-Zip, Adobe: Acrobat / Bridge / Creative Cloud / Distiller / Dreamweaver / Flash / Photoshop / Reader, Apache, Apache Tomcat, Apple: iCloud / iTunes / Mobile Device Support / QuickTime / Safari /*	

					Software Update, WebEx: Meeting Center / Productivity Tools, Citrix Receiver / Single Sign-On / Delivery Controller / GoToMeeting / Online Plugin / Provisioning Services / Virtual Delivery Agent / XenApp / XenDesktop, FileZilla, Foxit: Phantom PDF / Reader, Gimp, TightVNC, Google: Chrome Browser for enterprise / Drive / Picasa, Greenshot, KeePass, LibreOffice, ImgBurn, Microsoft: .NET / Azure / DirectX / Dynamics / Exchange Server / Exchange System Manager / Forefront / Internet Explorer / Internet Information Server / Lync / Lync Server / Office / Outlook / Power BI Desktop / Report Viewer / Search / Services for Unix / Sharepoint / Skype / Silverlight / System Center Operations Manager / System Center Virtual Machine Manager / SQL Server / Systems Management Server / Virtual Machine / Virtual PC / Virtual Server / Visual Basic / Visual C++ / Windows / Windows Defender / WSUS / Windows Mail / Kerberos, Firefox, Thunderbird, Notepad++, GeForce Experience, Opera, Oracle: OpenOffice / VM VirtualBox, Recuva, Prezi Desktop, RealVNC, PuTTY, Java, TeamViewer, PDF-Xchange, UltraVNC, VLC, VMware: Horizon View Client / Player / Tools / Workstation, WinSCP, Wireshark, Xmind) **F.** CERINŢE FAŢĂ DE DISK ENCRYPTION 1. Soluţie pentru managementul criptării discurilor pentru 100 calculatoare portabile: GravityZone Full Disk Encryption sau echivalentul. Soluţia trebuie să acopere următoarele funcţionalităţi minime: 1.1. Administrarea produsului trebuie să fie realizată din aceeaşi consolă de management ca şi soluţia de protecţie antivirus pentru mediul fizic (staţii şi servere), mediul virtual (VDI-uri şi servere virtuale), căsuţe de email Exchange şi dispozitive mobile (Android si iOS). 1.2. Clientul pentru disk encryption nu trebuie să fie ca un modul separat în cadrul clientului Antivirus. 1.3. Produsul trebuie să folosească mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows si FileVault pentru Mac OSX. 1.4. Produsul trebuie să cripteze hard diskurile staţiilor de lucru integral. 1.5. Produsul trebuie să impună autentificarea utilizatorului înainte de startarea sistemei de operare (pre-boot authentication). 1.6. Produsul trebuie să păstreze cheile de criptare pe acelaşi server de management al protecţiei antivirus, managementul cheilor utilizate să fie efectuat din aceeaşi consolă comună, inclusiv recuperarea rapidă a cheilor la solicitarea autorizată. 1.7. Produsul trebuie să ofere un raport complet asupra stării de criptare a dispozitivelor inclusiv: numele staţiei, IP-ul staţiei, sistemul de operare, ID-ul volumului/partiţiei, numele partiţiei, starea criptării partiţiei, tipul partiţiei: boot, non-boot, mărimea partiţiei în GB, ID-ul cheii de recuperare. 1.8. Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7 Enterprise (with TPM); Windows 8.1 Pro/ Enterprise; Windows 10 Pro/ Enterprise; WindowsServer 2008 R2 (withTPM); WindowsServer 2012/2012 R2, WindowsServer 2016, OSX 10.9/ 10.10 / 10.11/ 10.12	

					G. CERINŢE FAŢĂ DE SERVICIILE DE IMPLEMENTARE ŞI CONFIGURARE **1.** 1.1. Limba de comunicare şi documentare va fi limba română 1.2. Ofertantul selectat va livra şi instala licenţele pentru soluţia ofertată. 1.3. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluţia propusă, după care va asigura implementarea iniţială a soluţiei aplicative în mediul de producţie şi mediul de testare al clientului. 1.4. Ofertantul selectat va efectua configurarea iniţială a soluţiei, atât pentru mediul de producţie, cât şi mediul de testare. Prin configurare iniţială (Furnizorul) înţelege setarea tuturor parametrilor aplicabili în corespundere cu cerinţele (clientului), inclusiv configurarea şi instalarea soluţiei ofertate, setarea politicilor şi testarea înainte de a fi pusă în producţie. 1.5. În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările/personalizările agreate darea în exploatare a soluţiei. 1.6. Ofertantul va asigura integrarea soluţiei cu cel puţin următoarele aplicaţii terţe: 1.6.1. Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluţiei prin AD; 1.6.2. Integrarea cu platforma mobilă (telefoane, tablete) – pentru securizarea perimetrului de dispozitive mobile. 1.7. Ofertantul selectat va efectua instalarea soluţiei ofertate în întreaga infrastructură a Ministerului Apărării inclusiv la toţi utilizatorii finali (instalarea se va considera încheiată în momentul când toţi utilizatorii vor avea instalat agentul şi calculatorul va primi cel puţin o actualizare a bazelor şi a agentului) 1.8. La sfârşitul etapei, Ofertantul va face o demonstraţie a soluţiei şi a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanţă ale etapei de implementare. 1.9. După acceptanţa finală a soluţiei, va fi activată în mod automat opţiunea de garanţie post-implementare şi suport. Perioada de garanţie post-implementare şi suport va fi de 36 luni de la data activării acestei opţiuni. 1.10. Serviciile de garanţie post-implementare şi suport se referă la serviciile oferite de către Ofertantul selectat adiţional la serviciile de mentenanţă şi suport a licenţelor, oferite direct de către producătorul licenţelor. 1.11. Serviciile de garanţie post-implementare şi suport, vor include următoarele componente: 1.11.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; 1.11.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ; 1.11.3. Solicitărilor de schimbare a politicilor de securitate; 1.11.4. Solicitări de analiza şi corecţie a politicilor de securitate în cadrul companiei implementate. **H.** CERINŢELE FATA DE SERVICIILE DE INSTRUIRE	

					1. 1.1. Limba de comunicare şi documentare va fi limba română 1.2. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire şi transfer de cunoştinţe pentru grupurile ţintă în vederea formării setului de cunoştinţe necesar pentru a permite echipei instruite să preia menţinerea şi configurarea ulterioară a soluţiei, în conformitate cu necesităţile companiei. 1.3. Instruirea se va organiza pentru diferite grupuri ţintă la sediul Cumpărătorului. 1.3.1. Analist – nr. persoane stabilite de către client 1.3.2. Administrator - nr. persoane stabilite de către client 1.4. În acest sens, ca parte a ofertei, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum şi cuprinsul/agenda acestor instruiri. 1.5. În afara instruirilor ce ţin de utilizarea soluţiei, Ofertantul trebuie să efectueze şi sesiuni de instruire pentru echipa de menţinere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoştinţe şi competenţe, pentru a putea utiliza eficient instrumentele de configurare şi dezvoltare disponibile în cadrul soluţiei. 1.6. În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoştinţe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puţin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părţi. 1.7. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze şi să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: 1.7.1. Strategia Ofertantului cu privire la instruire şi programul de formare; 1.7.2. Structura şi componenţa pachetului de cursuri pentru formare şi a manualelor de studiu pentru fiecare categorie de utilizator; 1.7.3. Metodologia şi procedurile de evaluare şi control al eficienţei şi suficienţei sesiunilor de instruire. 1.8. În cadrul sesiunilor de instruire, Ofertantul va pune la dispoziţia Cumpărătorului întreg setul de documentaţie al soluţiei, care să cuprindă cel puţin următoarele componente: 1.8.1. Ghidurile administratorilor 1.8.2. Ghidurile de instalare şi configurare. 1.8.3. Fişierele surse pentru toate configurările şi personalizările realizate pe parcursul proiectului. ***Cerinţe minime de calificare a ofertanţilor:*** *1.7. Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanţă, inclusiv suport local din partea partenerului.* *1.8. Prezentare a minim 2 certificate tehnice al ofertantului;* *1.9. Lucrările de instalare, configurare, punerea în funcţiune a soluţiei trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.* *1.10. Ofertantul trebuie sa fie certificat ISO 9001 şi*	

					27001. Prezentarea documentelor justificate este obligatorie. *1.11. Prezentarea autorizării de la Producător (MAF);* *1.12. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de a oferi suport tehnic pe teritoriul R. Moldova;* *Termen livrare: pînă la 30 zile de la data intrării în vigoare a contractului, care include şi timpul lucrărilor de instalare, configurare şi punerea în funcţiune a soluţiei.*	
						833400,00

9. În cazul în care contractul este împărţit pe loturi un operator economic poate depune oferta: Pentru fiecare lot în parte.

10. Admiterea sau interzicerea ofertelor alternative: Nu se admite.

11. Termenii şi condiţiile de livrare/prestare/executare solicitaţi: Livrarea şi instalarea se va efectua la Centru comunicaţii şi informatică - or. Chişinău, şos. Hînceşti 84. Termenul de livrare – pînă la 30 zile de la data intrării în vigoare a contractului, care include şi timpul lucrărilor de instalare, configurare şi punerea în funcţiune a soluţiei.

12. Termenul de valabilitate a contractului: 31.12.2020

13. Contract de achiziţie rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): nu

14. Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): -

15. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora şi a criteriilor de selecţie; nivelul minim (nivelurile minime) al (ale) cerinţelor eventual impuse; se menţionează informaţiile solicitate (DUAE, documentaţie):

Nr. d/o	Descrierea criteriului/cerinţei	Mod de demonstrare a îndeplinirii criteriului/cerinţei:	Nivelul minim/ Obligativitatea
1.	Eligibilitatea ofertantului	DUAE - Formularul standard al Documentului Unic de Achiziţii European	Obligatoriu
2.	Propunerea financiară	Formularul ofertei (F 3.1) - cu aplicarea semnăturii electronice	Obligatoriu
		Specificaţii de preţ (F 4.2) - cu aplicarea semnăturii electronice	Obligatoriu
		Garanţia pentru ofertă – 1% din valoarea ofertei fără TVA - cu aplicarea semnăturii electronice	Obligatoriu
3.	Propunerea tehnică	Specificaţii tehnice (F 4.1) - cu aplicarea semnăturii electronice	Obligatoriu

16. Motivul recurgerii la procedura accelerată (în cazul licitaţiei deschise, restrânse şi al procedurii negociate) după caz: -

17. Tehnici şi instrumente specifice de atribuire: nu se va utiliza licitaţie electronică.

18. Condiţii speciale de care depinde îndeplinirea contractului: nu sunt.

19. Criteriul de evaluare aplicat pentru adjudecarea contractului: preţul cel mai scăzut.
Conform art. 26 alin.18, Legea nr. 131 din 03.07.2015, privind achiziţiile publice, în cazul în care două sau mai multe oferte sînt echivalente va fi aplicat un criteriu de atribuire suplimentar - capacitatea economică şi financiară (art. 18, lit. c), Legea 131/2015). Ofertantul clasat pe primul loc

va prezenta în termen de 3 zile, la solicitarea autorităţii contractante, documentele justificative actualizate prin care va demonstra îndeplinirea tuturor criteriilor de calificare şi selecţie, în conformitate cu informaţiile cuprinse în DUAE, după cum urmează:

Nr. d/o	Denumirea documentului	Descrierea documentului:	Nivelul minim/ Obligativitatea
1.	Certificat de atribuire a contului bancar	eliberată de banca deţinătoare de cont - cu aplicarea semnăturii electronice	Obligatoriu
2.	Certificat privind lipsa sau existenţa restanţelor faţă de bugetul public naţional	eliberat de Serviciul Fiscal de Stat, valabil la momentul prezentării (valabilitatea certificatului – conform cerinţelor Serviciului Fiscal de Stat al Min. Fin.) - cu aplicarea semnăturii electronice	Obligatoriu
3.	Dovada înregistrării persoanei juridice, în conformitate cu prevederile legale din ţara în care ofertantul este stabilit	Certificat/decizie de înregistrare a întreprinderii/extras din Registrul de Stat al persoanelor juridice - cu aplicarea semnăturii electronice. Operatorul economic nerezident va prezenta documente din ţara de origine care dovedesc forma de înregistrare/atestare ori apartenenţa din punct de vedere profesional	Obligatoriu
4.	Prezentarea de dovezi privind conformitatea produselor, identificată prin referire la specificaţii sau standard relevante	Certificat ISO 27001:2013 şi Certificat ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice.	Obligatoriu
5.	Actul care atestă dreptul de a livra bunuri/lucrări/servicii	Autorizaţie de la producător (MAF - Manufacturer Authorization Form) - Copie – confirmat cu aplicarea semnăturii electronice	Obligatoriu
		Certificat/Autorizaţie de la producător care conferă dreptul de a oferi suport tehnic pe teritoriul R. Moldova - confirmat cu aplicarea semnăturii electronice.	Obligatoriu pentru lotul nr.2
6.	Certificat de garanţie	Certificat de garanţie şi service postgaranţie pe o perioada de minim 36 luni; – original confirmat cu ştampila umedă a participantului.	Obligatoriu pentru lotul nr.2 la livrare
7.	Certificat de training al inginerului din cadrul companiei ofertante	Confirmat prin aplicarea semnăturii electronice	Obligatoriu

20. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum şi ponderile lor: -

21. Termenul limită de depunere/deschidere a ofertelor:conform ***SIA "RSAP"***

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

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul ***SIA "RSAP"***

23. Termenul de valabilitate a ofertelor: 45 zile.

24. Locul deschiderii ofertelor: conform ***SIA "RSAP"***

Ofertele întârziate vor fi respinse.

25. Persoanele autorizate să asiste la deschiderea ofertelor:

Ofertanţii sau reprezentanţii acestora au dreptul să participe la deschiderea ofertelor, cu excepţia cazului când ofertele au fost depuse prin SIA "RSAP".

26. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: De stat

27. Respectivul contract se referă la un proiect şi/sau program finanţat din fonduri ale Uniunii Europene: -

28. Denumirea şi adresa organismului competent de soluţionare a contestaţiilor:
Agenţia Naţională pentru Soluţionarea Contestaţiilor
Adresa: mun. Chişinău, bd. Ştefan cel Mare şi Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email:022-820 652, 022 820-651, contestatii@ansc.md

29. Data (datele) şi referinţa (referinţele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunţul respective (dacă este cazul): -

30. În cazul achiziţiilor periodice, calendarul estimat pentru publicarea anunţurilor viitoare:-

31. Data publicării anunţului de intenţie sau după caz precizarea că nu a fost publicat un astfel de anunţ: BAP nr.6 din 11.02.2020

32. Data transmiterii spre publicare a anunţului de participare:conform SIA RSAP

33. În cadrul procedurii de achiziţie publică se va utiliza/accepta:

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
depunerea electronică a ofertelor sau a cererilor de participare	Da
sistemul de comenzi electronice	Nu
facturarea electronică	Da
plăţile electronice	Da

34. Contractul intră sub incidenţa Acordului privind achiziţiile guvernamentale al Organizaţiei Mondiale a Comerţului (numai în cazul anunţurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): nu

35. Alte informaţii relevante:
1. Contractul va fi însoţit de o Garanţie de bună execuţie, în mărime de 5% din valoarea contractului, inclusiv TVA, (emisă de o bancă comercială, cu termen de valabilitate pînă la 31.12.2020) conform formularului F 3.3 din documentaţia standard pentru realizarea achiziţiilor publice de bunuri, sau prin transfer la contul autorităţii contractante, conform următoarelor date bancare:
Beneficiarul plăţii: **Agenţia Asigurare Resurse şi Administrare Patrimoniu a Ministerului Apărării**
Denumirea Băncii: **Ministerul Finanţelor – Trezoreria de Stat**
Codul fiscal: **1006601001229**
Cod IBAN: **MD28TRPCAA518410A00572AA**
cu nota "Pentru garanţia de buna execuţie a contractului".
2. Ofertele ce depăşesc cu 30% valoarea estimată a achiziţiei nu vor fi acceptate.

Conducătorul grupului de lucru: _____ **L.Ş.**