Proiectul PNUD "Building e-Governance in Moldova - 2"

CERERE DE OFERTĂ

Ministerul Afacerilor Interne al Republicii Moldova și Programul Națiunilor Unite pentru Dezvoltare invită companiile interesate pentru a prezenta oferte conform termenilor de referinţă de mai jos.

Termeni de referinţă

Elaborarea Sistemului Informațional “Registrul de Stat al Armelor”

Chișinău 2012

Cuprins

1. Generalități

1.1. Context

Proiectul "Building e-Governance in Moldova - 2" finanţat si implementat de Proiectul Naţiunilor Unite pentru Dezvoltare (PNUD) în colaborare cu Ministerul Afacerilor Interne (MAI) al Republicii Moldova şi alte agenţii de stat si internaţionale, acordă asistenţă Guvernului Republicii Moldova în scopul eficientizării activităţii de supraveghere asupra circulaţiei armelor şi muniţiilor cu destinaţie civilă deţinute de persoane fizice şi juridice, ajustării cadrului legislativ şi normativ la cerinţele Convenţiei Europene cu privire la controlul achiziţionării şi deţinerii armelor de foc de către particulari (ratificată prin Legea nr. 1578-XV din 20 decembrie 2002), instituirii măsurilor de evidenţă şi control şi realizării obiectivelor corespunzătoare condiţiilor actuale şi de perspectivă.

Unul din obiectivele proiectului este de a susține Ministerul Afacerilor Interne al Republici Moldova în crearea și implementarea Registrului de stat al armelor (RSA) - sistem complex de prelucrare a datelor cu privire la evidența armelor, a deținătorilor legali de arme, precum și a operațiunilor cu arme și muniții, organizat la nivelul MAI și administrat de structura ce coordoneaza domeniul de activitate.

Suportul legislativ al acestei iniţiative este asigurat de prevederile Decretului Președintelui Republicii Moldova nr.1743-III din 19 martie 2004 „Privind edificarea societăţii informaţionale în Republica Moldova", Hotărârii Guvernului (HG) nr. 632 din 8 iunie 2004 „Privind aprobarea Politicii de edificare a societăţii informaţionale în Republica Moldova", HG nr. 255 din 09.03.2005 „Privind Strategia Naţională de edificare a societăţii informaţionale", HG nr. 634 din 06.06.2007 cu privire la aprobarea Concepţiei Sistemului informaţional automatizat „Registrul de stat al armelor", Legii nr. 110-XIII din 18 mai 1994 cu privire la arme (Monitorul Oficial al Republicii Moldova, 1994, nr. 4, art. 43) şi pct. 2 al Hotărîrii Guvernului nr. 1202 din 17 octombrie 2006 "Cu privire la aprobarea Concepţiei Sistemului informaţional integrat al organelor de drept" (Monitorul Oficial al Republicii Moldova, 2006, nr. 168-169, art.1293).

Implementarea Sistemului informaţional automatizat "Registrul de stat al armelor" se va efectua în cadrul Programului de dezvoltare şi automatizare a procesului de schimb informaţional între participanţii la Sistemul informaţional integrat automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni, aprobat prin Hotărîrea Guvernului nr. 770 din 6 iulie 2004.

1.2. Perioada implementării

Durata realizării Proiectului – 4 luni din momentul semnării contractului.

1.3. Obiective

Elaborarea Sistemului Informaţional Automatizat „Registrul de Stat al armelor", care să conţină și să prelucreze date cu privire la evidența

- armelor letale și neletale,
- deținătorilor legali de arme, muniții și a datelor privind documentele de autorizare, deținere, folosire și transfer,
- armurierilor/reparatorilor și a datelor privind documentele de autorizare, deținere, folosire și transfer,
- poligoanelor de tragere, tirurilor.

1.4. Scopuri

Prin crearea și implementarea „Registrului de Stat al armelor" vor fi atinse următoarele scopuri:

- evidenţa şi controlul unic centralizat asupra circulaţiei armelor în Republica Moldova;

- colectarea şi actualizarea informaţiei despre arme, starea lor tehnică, despre dreptul de proprietate şi alte drepturi patrimoniale asupra lor şi despre modificările acestor drepturi, despre titularii de drept şi documentele ce stabilesc un drept, sub forma creării unei bănci de date de informaţii integrate, destinate organizării accesului operativ la aceasta;
- acordarea de ajutor organelor centrale de specialitate ale administraţiei publice şi autorităţilor administraţiei publice locale în eficientizarea realizării politicii de stat în domeniul evidenţei şi controlului asupra circulaţiei armelor;
- prevenirea şi contribuirea la descoperirea operativă a infracţiunilor şi a altor încălcări, săvîrşite cu utilizarea armelor;
- sporirea calităţii asigurării informaţionale a activităţii organelor de drept;
- oferirea posibilităţii de interacţiune informaţională şi de colaborare în cadrul schimbului informaţional interstatal şi internaţional;
- asigurarea identificării operative şi depline a armelor, care se află în circulaţie pe teritoriul Republicii Moldova, prin organizarea accesului la banca de date integrată prin canalele de legătură în timp real şi interpelare amînată (poşta electronică).

1.5. Principii

Registrul de stat al armelor va fi creat şi implementat în baza principiilor legalităţii, respectării drepturilor omului, temeiniciei, integrităţii, plenitudinii şi veridicităţii datelor, identificării de stat a obiectelor de înregistrare, securităţii informaţionale, modularităţii, flexibilităţii şi scalabilităţii,

1.6. Baza juridico-normativă

Baza juridico-normativă a RSA o constituie legislaţia în vigoare a Republicii Moldova şi tratatele internaţionale la care Republica Moldova este parte, inclusiv:

1. Constituţia Republicii Moldova.
2. Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal cu Protocolul adiţional. Strasbourg, 1981, http://datepersonale.md/md/international003/
3. Codul vamal, adoptat prin Legea nr.1149-XIV din 20 iulie 2000.
4. Legea nr. 110-XIII din 18 mai 1994 cu privire la arme.
5. Legea cu privire la registre Nr.1320-XIII din 25.09.97. Monitorul Oficial al R.Moldova nr.77-78 din 27.11.1997
6. Legea nr.451-XV din 30 iulie 2001 privind licenţierea unor genuri de activitate.
7. Legea nr. 1578-XV din 20 decembrie 2002 pentru ratificarea Convenţiei europene cu privire la controlul achiziţionării şi deţinerii armelor de foc de către particulari.
8. Legea nr.186-XV din 24 aprilie 2003 cu privire la evaluarea conformităţii produselor.
9. Legea nr.467-XV din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat.
10. Legea Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal. Monitorul Oficial Nr. 170-175
11. Hotărîrea Guvernului nr. 840 din 26 iulie 2004 „Cu privire la crearea Sistemului de telecomunicaţii al autorităţilor administraţiei publice" (Monitorul Oficial al Republicii Moldova, 2004, nr. 130, art.1013);
12. Hotărîrea Guvernului nr. 44 din 18 ianuarie 1995 "Cu privire la măsurile de realizare a Legii nr. 110-XIII din 18 mai 1994.
13. Hotărîrea Guvernului nr. 711 din 23 iunie 2006 "Cu privire la Comisia republicană pentru evaluarea, bonificarea şi rebutarea armelor individuale".
14. Hotărîrea Guvernului nr. 126 din 15 februarie 2000 "Cu privire la aprobarea Listei cu tipurile de arme şi muniţiile aferente pasibile de vînzare persoanelor fizice şi juridice".
15. Hotărîrea Guvernului nr. 1173 din 19 decembrie 1997 "Cu privire la raportarea unor modele de arme la armele individuale.
16. Hotărîrea Guvernului nr. 1010 din 31 octombrie 1997 „Cu privire la aprobarea Regulilor comerţului de consignaţie".
17. HG nr. 634 din 06.06.2007 cu privire la aprobarea Concepţiei Sistemului informaţional automatizat „Registrul de stat al armelor".

18. Hotărîre de guvern Nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal. Monitorul Oficial Nr. 254-256, 24.12.2010, art Nr : 1282.
19. Reglementare tehnică „Procesele ciclului de viaţă al software-ului” RT 38370656- 002:2006.

1.7. Conţinutul lucrărilor

În baza Concepţiei Sistemului informaţional automatizat „Registrul de stat al armelor” compania câştigătoare urmează să propună/elaboreze o soluţie software de evidenţă centralizată şi control al circulaţiei armelor și a munițiilor, inclusiv evidenţa armelor mici din gestiunea structurilor de stat ce au în competenţa lor subdiviziuni militarizate, a datelor gestionate de structura centrală din MAI și de structurile teritoriale de arme, explozivi din comisariatele raionale de poliție, soluție care va asigura administrarea la nivel statal a activității informatice de exploatare în interes operativ și analitic a datelor prevăzute în categoriile de evidențe conform p. 1.3.

Companiile participante în concurs vor include în ofertă lista și specificațiile echipamentelor tehnice. Prețul echipamentelor nu va fi inclus în prețul ofertei.

2. Funcțiile sistemului

Registrul de stat al armelor va asigura îndeplinirea următoarelor funcții de bază:
1. formarea bazei de date;
2. organizarea administrării informaţionale a bazei de date;
3. asigurarea calităţii informaţiei;
4. garantarea securității informaţionale.

2.1. Formarea bazei de date

La formarea bazei de date funcţiile principale sunt:
- punerea primară la evidenţă,
- actualizarea datelor,
- scoaterea de la evidenţă (transferarea datelor în arhivă).

Punerea primară la evidenţă constă în atribuirea unui identificator unic de evidenţă a obiectului informaţional (arma, proprietarul sau beneficiarul armei, armurierul, poligonul, tirul) şi introducerea în baza de date a Sistemului a unui volum stabilit de date despre el.

Actualizarea datelor sistemului constă în înnoirea sistematică a bazei de date la modificarea sau completarea datelor asociate obiectelor de evidenţă.

Scoaterea de la evidenţă şi transferarea datelor în arhivă se efectuează prin aplicarea unei marcări sau transformări speciale în baza de date, necesare în cazul cercetărilor istorice sau procesării analitice on-line.

Toate modificările în Sistem se păstrează în ordine cronologică. Funcţiile menţionate mai sus sînt îndeplinite la organizarea colectării datelor despre arme şi despre titularii lor de drept în timpul producerii, vînzării, transmiterii, achiziţionării, păstrării, portului, transportării, inclusiv tranzitului, folosirii, confiscării şi distrugerii, exportului şi importului, precum şi la introducerea în şi scoaterea de pe teritoriul Republicii Moldova a exemplarelor unice de arme.

2.2. Organizarea administrării bazei de date

Schimbul informaţional de date între sistemele informaţionale automatizate departamentale se efectuează în baza unui regulament, aprobat de către toţi participanţii la Sistemul informaţional integrat al organelor de drept.

Informaţia din baza de date este oferită de către deţinătorul Registrului de stat al armelor în modul stabilit de legislaţia în vigoare. Informaţia care se conţine în RSA nu este publică, iar divulgarea ei neautorizată se pedepseşte conform legii.

2.3. Asigurarea calităţii informaţiei

Calitatea informaţiei va fi asigurată prin crearea şi menţinerea sistemului de calitate, bazat pe abordarea procesuală în conformitate cu Standardul naţional SM EM ISO 9001:2002 „Sisteme de management al calităţii. Cerinţe".

2.4. Garantarea securității informaționale

Securitatea informațională va fi asigurată prin elaborarea și implementarea unui sistem de management în conformitate cu standardele internaționale securității informaționale ISO 27000 și cerințele Hotărîrii de guvern Nr. 1123 din 14.12.2010.

2.5. Blocurile funcționale

Setul recomandabil de blocuri funcționale este prezentat în Concepţiei Sistemului informaţional automatizat „Registrul de stat al armelor" (se anexează). Participanții la concurs pot propune viziuni proprii, dar care vor include toate funcționalitățile menționate în Concepție.

3. Cadrul organizatoric

3.1. Posesorul RSA

Posesor al Registrului de stat al armelor este Ministerul Afacerilor Interne.

3.2. Deșinătorul RSA

Deținător al Registrului de stat al armelor este Ministerul Afacerilor Interne.

3.3. Registratorii RSA

Registratori ai Registrului de stat al armelor sunt Ministerul Afacerilor Interne și armurierii licențiați.

Ministerul Afacerilor Interne este responsabil de evidența:

- armelor (inclusiv celor mici din gestiunea structurilor de stat ce au în componenţă subdiviziuni militarizate sau speciale) aflate în circulaţie pe teritoriul Republicii Moldova;
- proprietarilor şi beneficiarilor de arme, precum şi a condiţiilor de apariţie şi încetare a drepturilor corespunzătoare;
- documentelor eliberate, aferente circulaţiei armelor;
- verificărilor efectuate în scopul controlului asupra respectării regulilor de comercializare, achiziţionare, păstrare, port, transportare şi folosire a armelor.

Armurierii licențiați în calitate de registratori sunt responsabili de introducerea informațiilor despre armele vândute, reparate, întoarse pe garanție, schimbate, muniții, actele prezentate la eliberarea armelor, munițiilor și alte informații în conformitate cu cadrul normativ-legal.

3.4. Documentele sistemului

Documentele RSA vor fi din următoarele categorii: documente ce stabilesc un drept, documente de premiere, contracte de donaţie, certificat de moştenitor, documente prin care se confirmă înregistrarea de către Ministerul Culturii a armelor în fondul unui muzeu sau includerea armelor în

colecţie specială, acte de identitate şi licenţe, documente tehnice, documente tehnologice (blanchete, chestionare şi alți suporți de informaţie despre arme).

4. Resursele informaționale

4.1. Obiectele informaționale

Resursa informaţională a RSA este reprezentată de totalitatea obiectelor informaţionale determinată de destinaţia sistemului şi include:

- arme cu destinaţie civilă şi arme mici din gestiunea structurilor de stat ce au în competenţa lor subdiviziuni militarizate sau speciale;
- titularii de drepturi la arme:
  - persoane fizice (obiectul informaţional este împrumutat din Registrul de stat al populaţiei);
  - persoane juridice (obiectul informaţional este împrumutat din Registrul de stat al unităţilor de drept);
- drepturi:
  - de proprietate;
  - de folosinţă;
- verificări;
- documente din următoarele categorii:
  - ce stabilesc un drept;
  - de autorizare;
  - documentaţia tehnică.

Pe lîngă aceasta, resursa informaţională trebuie să conţină două obiecte informaţionale obligatorii: evenimentul şi formularul.

4.2. Identificarea obiectelor

Identificator al obiectului informaţional „armă” este numărul de identificare de stat al armei (IDAR), reprezentînd o succesiune strict determinată din 10 simboluri, în care:

- primul simbol - constituie indicile sistemic interior al obiectului informaţional (pentru arme - 7);
- simbolurile 2 şi 3 - ultimele două cifre din anul atribuirii numărului de identificare;
- simbolurile 4 şi 5 - codul organului de poliţie care a înregistrat arma;
- simbolurile 6 până la 10 - numărul de ordine de înregistrare a armei la organul de poliţie.

Identificator al obiectului informaţional „titular de drepturi” este numărul de identificare de stat al persoanei fizice (IDNP) - pentru persoane fizice sau numărul de identificare de stat al unităţii de drept (IDNO) - pentru persoane juridice.

Identificator al obiectului informaţional „dreptul” este cheia combinată < IDAR> +identificatorul posesorului dreptului.

Identificator al obiectului informaţional „verificarea” este numărul lui de identificare (ID), care reprezintă o succesiune strict determinată din 8 simboluri, în care:

- primele două simboluri constituie ultimele două cifre ale anului atribuirii numărului de identificare;
- restul simbolurilor reprezintă numărul de ordine al verificării în anul respectiv.

Identificator al obiectului informaţional “document” este cheia combinată „tipul documentului” + „numărul” + “seria”.

Identificator al obiectului informaţional „eveniment” este numărul lui de ordine.

Identificator al obiectului informaţional „formular” este numărul lui de ordine.

4.3. Scenarii de bază

Scenariile de bază realizează funcţiile RSA legate de administrarea informaţiei şi se divizează în următoarele grupe conform obiectelor informaționale:

a) Pentru obiectul informaţional „armă”:

Punerea primară la evidenţă se efectuează:

- la eliberarea autorizaţiilor pentru importul armelor pe teritoriul Republicii Moldova de către subdiviziunile Ministerului Afacerilor Interne:
  - pentru aflare provizorie (competiţii sportive, vînătoare);
  - pentru importul exemplarelor unice de arme;
  - persoanelor juridice pentru comercializarea sau utilizarea ulterioară a armelor;
  - pentru transportul armelor în tranzit, prin teritoriul Republicii Moldova; a persoanelor fizice pentru uz personal al armelor;
- la eliberarea armelor de la depozitele unităţilor militare ale Ministerului Apărării, care urmează a fi utilizate cu destinaţie civilă;
- la perfectarea autorizaţiilor pentru dreptul de expunere sau de păstrare a armelor în colecţie;
- la desfăşurarea testărilor de certificare a armelor produse pe teritoriul Republicii Moldova.

Actualizarea datelor se efectuează la:

- transportarea armelor peste frontiera de stat a Republicii Moldova, inclusiv a armelor care traversează frontiera prin tranzit, realizată de către Serviciul Vamal;
- perfectarea autorizaţiei de păstrare sau portarmă;
- examinarea tehnică a armelor;
- înlocuirea documentelor;
- schimbarea proprietarului sau beneficiarului armei sau a cotei-părţi a proprietăţii lui;
- pierderea sau furtul armei;
- anularea autorizaţiilor eliberate anterior;
- confiscarea armelor.

Actualizarea datelor prin modificare poate fi efectuată numai de persoane abilitate. Pentru această acţiune sînt utilizate aceleaşi forme de ecran ca şi în cazul introducerii primare a datelor. Modificările efectuate nu servesc motiv pentru vizualizarea imediată a schimbărilor introduse.

Sistemul trebuie să asigure înregistrarea modificărilor efectuate precum şi înştiinţarea persoanelor autorizate cu dreptul de decizie. Persoana autorizată vizualizează toate modificările fără decizie înregistrate în sistem şi acceptă sau refuză schimbările propuse. Lista schimbărilor înregistrate include doar operaţiunile fără decizie. Modificările sînt vizualizate în RSA imediat după acceptarea lor de către o persoană autorizată.

Este obligatoriu ca în sistem să fie înregistrată istoria fiecărei modificări (data modificării, autorul modificării, descrierea, data aprobării sau refuzului, autorul deciziei, motivul).

Scoaterea de la evidenţă se efectuează la:

- scoaterea definitivă a armelor din ţară, cu confirmarea ulterioară de către instituţiile vamale a faptului transportării lor peste hotare;
- distrugere.

b) Pentru obiectul informaţional „titular de drepturi”:

Punerea primară în evidenţă se efectuează la apariţia dreptului de proprietate (folosinţă).

Actualizarea datelor se efectuează la schimbarea domiciliului proprietarului armei de foc.

Scoaterea din evidenţă se efectuează la încetarea dreptului de proprietate (folosinţă).

c) Pentru obiectul informaţional „dreptul”:

Punerea primară în evidenţă se efectuează la apariţia dreptului de proprietate (folosinţă).

Actualizarea datelor se efectuează la modificarea sau limitarea dreptului de proprietate (folosinţă).

Scoaterea din evidenţă se efectuează la încetarea dreptului de proprietate (folosinţă).

d) Pentru obiectul informaţional “verificare”:

Punerea primară în evidenţă are loc la efectuarea verificării.

Actualizarea datelor se efectuează la amînarea termenului de verificare, contestarea deciziilor luate conform rezultatelor verificării.

e) Pentru obiectul informaţional "document":

Punerea primară în evidenţă se efectuează la:
- confecţionare;
- evidenţa documentelor din alte sisteme.

Actualizarea datelor se efectuează la:
- schimbarea statutului documentului;
- schimbarea termenului de valabilitate.

Scoaterea din evidenţă se efectuează la:
- distrugere;
- scoaterea definitivă peste hotare.

f) Pentru obiectele informaţionale „eveniment" şi „formular":

Punerea primară în evidenţă se efectuează la înregistrarea evenimentului, concomitent se perfectează formularul corespunzător.

Actualizarea datelor se efectuează la luarea deciziilor corespunzătoare cu privire la formularul respectiv de către persoanele responsabile la toate etapele lanţului tehnologic de prelucrare a informaţiei (totodată, în formular se fac menţiunile corespunzătoare).

Scoaterea din evidenţă se efectuează la anularea evenimentului.

4.4. Căutarea informaţiei

Sistemul trebuie să permită căutarea eficientă a informaţiei stocate şi procesate în RSA. Sunt stabilite următoarele cerinţe referitor la căutare:
- menţinerea listei de criterii de căutare;
- listele de căutare sînt bazate pe structura informaţiei privind obiectele informaţionale;
- căutare simplă şi pe criterii combinate (utilizînd operaţiile logice AND şi/sau OR);
- căutare multi-nivel (căutare prin intermediul unei operaţiuni de căutare anterioare);
- trecerea la profilul obiectului din sistem în regim de redactare din rezultatul căutării;
- asigurarea unui mecanism de exportare a datelor obţinute.

4.5. Raportarea

Funcţionalitatea de raportare urmează să asigure vizualizarea şi accesul la lista rapoartelor predefinite, executarea lor, imprimarea rezultatelor sau exportul lor, precum şi administrarea. Lista rapoartelor predefinite se organizează în forma unei structuri ierarhice multi-nivel. Administrarea acesteia se face prin interfaţa specială de administrare, care permite modificarea denumirii, schimbarea locului de amplasare în structura ierarhică sau ştergerea unui raport selectat sau a unui grup de rapoarte. De asemenea, interfaţa poate fi utilizată pentru crearea unui grup nou. Accesul la aceste operaţiuni este acordat doar utilizatorilor cu rolul Administrator.

Rapoartele noi vor fi create cu ajutorul unui instrument de gestionare a machetelor de rapoarte. Acest instrument va permite crearea unei machete noi, modificarea ei, crearea machetei în baza uneia deja existente, ştergerea machetei, precum şi crearea unui raport în baza machetei selectate. Accesul la aceste operaţiuni este acordat utilizatorilor cu rolurile Supervizor sau Administrator.

Sistemul trebuie să asigure vizualizarea rezultatelor executării unei machete. La executare utilizatorul va fi invitat să introducă valorile pentru variabilele definite în machetă.

Rezultatul executării va fi un raport generat şi/sau lista mesajelor de avertizare şi/sau lista greşelilor de executare. Numai după executarea reuşită va fi posibilă crearea unui raport şi publicarea lui în lista de rapoarte. Numai rapoartele publicate vor fi disponibile pentru utilizatorii autorizați. La executarea operaţiunii de publicare pot fi definite drepturi de acces individuale (nu obligator bazate pe rolurile din sistem).

Utilizatorii vor putea vedea doar rapoartele la care au drepturi de acces.

În cursul implementării Elaboratorul este obligat să includă în SIA RSA următoarele rapoarte predefinite:

- Informaţii privind organizaţiile deținătoare de arme,
- Dinamica mișcării armelor pe organizaţii, tipuri de arme, muniții etc.,
- Raport după scopuri,
- Raport după categorie,
- Raport după data de înregistrare,
- Extras din Registru,
- Raport teritorial.

Numărul total de rapoarte predefinite va de aproximativ 20, iar lista finală va fi stabilită în Sarcina Tehnică.

4.6. Datele incluse în RSA

Datele reprezintă seturi de atribute ale obiectelor informaționale și includ:

a) date de identificare ale armei și date privind verificarea tehnică,
b) date despre modelele de arme,
c) date despre titularul de drepturi,
d) date despre drepturi,
e) date despre verificare,
f) date despre documente,
g) date despre eveniment,
h) date despre formular,
i) date despre locul (adresa şi statutul) unde se păstrează arma.

Datele incluse în RSA sunt prezentate în Concepția SIA RSA și vor fi concretizate în Sarcina Tehnică.

4.7. Accesul la RSA și interacţiunea cu alte sisteme informaţionale

Pe plan intern structurile operative din cadrul MAI vor putea consulta Registrul de Stat al Armelor în interes operativ, pe niveluri de securitate. Structurile operative din MAI, care vor avea acces la datele inscrise in Registrul de Stat al Armelor vor fi stabilite pe parcursul realizării proiectului. Elaboratorul trebuie să pună la dispoziția Beneficiarului instrumente de lucru cu această listă.

Cetățenii vor dispune de posibilitatea depunerii cereri de procurare a unei arme prin Internet. Accesul cetățenilor va fi realizat prin servicii electronice folosind ghișeul unic asigurat de portalul guvernamental. Până la lansarea finală a ghișeului unic ieșirea la acest serviciu trebuie să fie asigurată de pe site-ul public www.mai.gov.md.

Pe plan extern RSA va include instrumente și mecanisme de conectare cu structurile similare din statele membre ale Uniunii Europene pentru schimbul reciproc de date și informații privind circulația armelor și muniților din Republica Moldova în spațiul Uniunii Europene și invers. Accesul structurilor similare din statele membre ale Uniunii Europene pentru consultarea RSA se va face pe niveluri de acces și securitate stabilite, potrivit legii.

SIA RSA va avea acces la resursele informaţionale ale următoarelor sisteme informaţionale automatizate:

a) SIA „Registrul de stat al populaţiei”, care acordă acces la datele personale ale titularilor de drepturi la arme şi la actele lor de identitate;
b) SIA „Registrul de stat al unităţilor de drept”, care acordă acces la datele de înregistrare a titularilor de drepturi la arme şi la documentele lor de înregistrare;
c) SIA „Registrul de stat al blanchetelor de strictă evidenţă şi al timbrelor de acciz”, care acordă accesul la datele despre blanchetele de strictă evidenţă, utilizate la întocmirea documentelor;
d) Sistemul informaţional al Serviciului Vamal, care acordă acces la datele despre armele transportate peste frontiera de stat şi documentele care au fost eliberate la import;
e) SIA „Registrul judiciar”, care acordă accesul la datele despre deciziile judecătoreşti intrate în vigoare, privind drepturile la arme;
f) SIA „Registrul informaţiei criminale şi criminologice”, care acordă acces la datele despre armele sustrase, pierdute, depistate, confiscate, predate, căutate, despre antecedentele penale ale persoanelor, tragerea la răspundere administrativă, despre persoanele aflate în căutare sau în privinţa cărora s-a pornit urmărirea penală, precum şi la datele despre caracteristicile balistice individuale ale cartuşelor şi tuburilor pentru încercare trase, ale armelor confiscate de la locul crimei;
g) Sistemul integrat informaţional medical al Ministerului Sănătăţii, care acordă acces la datele despre existenţa sau lipsa bolilor psihice, abuzul de alcool, folosirea de către persoane, în scopuri nemedicale, a substanţelor narcotice (psihotrope);

Prin protocoale de colaborare vor fi stabilite regulile și procedurile prin care se realizează schimbul de date între RSA și alte autorități, inclusiv MAEIE, Departamentul Vamal etc. Pentru interacțiune vor fi folosite serviciile web și canalele vpn (aproximativ 50 canale vpn).

5. Cerințe generale față de sistem

5.1. Arhitectura sistemului

Sistemul va fi elaborat în baza tehnologiilor web internet/intranet. Arhitectura RSA va respecta exigențele schemei-tip a infrastructurii informaţionale de comunicaţii electronice a SIA de Stat şi va fi formată din două niveluri: central şi regional.

Partea Server este instalată în Data Center al MAI şi include Serverul Web, Serverul Aplicaţii şi Serverul bazei de date. Serverul Web va asigura comunicarea utilizatorilor cu RSA pe baza protocolului http(s). Serverul de baze de date va conţine toată informaţia păstrată şi prelucrată de sistem. Serverul Aplicaţii va asigura logica business-proceselor, regulilor business şi efecutarea serviciilor prestate în cadru RSA. Arhitectura descrisă nu impune implementarea acestor aplicaţii pe servere dedicate.

Pentru accesul la sistem utilizatorul va avea nevoie doar de un browser Internet. Interfeţele utilizatorului şi funcţionarea corectă trebuie să fie asigurate, cel puţin, pentru următoarele aplicaţii: Internet Explorer 7.0+, Mozilla Firefox 2.0+, Opera 9.0+, GoogleChrome.

Accesul utilizatorilor din cadrul aparatului central al MAI va fi efectuat prin reţeaua locală sau canale vpn. Utilizatorii din alte organe ale administraţiei publice vor accesa serviciile SIA RSA prin reţeaua Centrului de telecomunicaţii speciale sau prin canale vpn.

Nivelul regional este amplasat în centrele raionale, în încăperile comisariatelor de poliţie. Funcţia de bază a acestui nivel este colectarea informaţiei. Legătura se va face prin canale vpn folosind un web browser.

5.2. Complexul tehnic de program

Lista produselor software şi a mijloacelor tehnice, utilizate la crearea infrastructurii informaţionale și de telecomunicaţii a SIA RSA, este întocmită de către Elaborator împreună cu grupul de lucru din partea MAI. Soluțiile program de tipul open source și echipamentele din categoria standardelor deschise vor avea prioritate.

6. Securitatea informaţională

6.1. Organizarea accesului

Accesul la sistem este permis numai în urma autentificării şi autorizării. Fiecare persoană va deţine un cont personal. Este interzisă utilizarea aceloraşi conturi de mai multe persoane. Autentificarea se face pe baza numelui de utilizator şi parolă.

Informaţia despre utilizatori se păstrează în baza de date cu indicarea obligatorie a datelor personale ale persoanei. Aceste date includ:

- cod utilizator (login name, username)
- nume utilizator;
- data înregistrării;
- IDNP;
- datele de identificare (parola în format protejat);
- adresa e-mail;
- acces cu adresa IP vpn;
- informaţia de contact.

În calitate de identificator unic va servi cheia combinată (login name)+IDNO/IDNP. Parola utilizatorului este păstrată în formă protejată (algoritm unidirecţional, de exemplu, MD5). Nu se permite stocarea datelor despre utilizatori în format deschis. Sistemul obligatoriu trebuie să asigure politica de gestiune a parolelor, cel puţin referitor la următoarele valori:

- lungimea parolei;
- complexitate (combinaţia caracterelor, cifrelor şi simbolurilor speciale);
- termenul de expirare (timpul maxim de utilizare a parolei neschimbate);
- numărul ciclurilor de nerepetare a parolei utilizate.

Accesul la sistem din exterior se face de utilizatorii, care au drepturi suficiente, definite în profilul clientului. Accesul la parametrizarea datelor de gestiune a conturilor, precum şi însăşi gestiunea conturilor, va fi permis doar pentru rolul Administrator. În acelaşi timp, fiecare din utilizatori are drepturi de schimbare a parolei şi a datelor personale. Acest mecanism presupune introducerea informaţiei, notificarea Administratorului şi aprobarea schimbărilor de către Administrator în urma verificărilor efectuate.

Pe lîngă datele personale ale utilizatorilor, în baza de date vor exista tabele separate pentru administrarea accesului la informaţie. Aceste tabele vor conţine informaţii despre utilizator şi rolul sau rolurile acordate în cadrul RSA, precum şi drepturile speciale ale utilizatorilor.

Este obligatoriu ca toate schimbările la obiectele din sistem să fie înregistrate în tabele speciale, cu indicarea obiectului, acţiunilor efectuate (introducerea informaţiei, modificarea, ştergerea), datei şi orei, utilizatorului, adresei IP, valorilor precedente şi cele noi. Trebuie înregistrate toate tentativele de acces nereuşit. Accesul la această informaţie (loguri) este permis doar pentru Administrator.

Accesul la sistem va fi organizat în formă de sesiune. Sesiunea utilizatorului trebuie să fie blocată după expirarea unui anumit termen de inactivitate (session timeout). În acest caz utilizatorul va fi obligat să repete procedura de conectare în RSA.

Pentru protecţia datelor trebuie asigurate alte măsuri tehnico-organizatorice, precum configurarea adecvată a reţelei, protecţia staţiilor de lucru şi politici interne de securitate.

6.2. Cerinţe privind integritatea informaţiei

În scopul asigurării integrităţii informaţiei din RSA sînt stabilite următoarele cerinţe:

- utilizarea obligatorie a mecanismelor tranzacţiilor;
- utilizarea funcţiilor şi procedurilor stocate;

- interfaţa utilizatorului trebuie să prezinte în mod unic marcarea cîmpurilor obligatorii în diverse forme electronice.

Interfaţa utilizatorului trebuie asigurată în limbile română, rusă şi engleză. Toate denumirile şi mesajele trebuie realizate sub formă de resurse, cu interfaţa adecvată pentru asigurarea existenţei traducerilor şi actualizarea lor, precum şi istoria creării şi modificărilor.

Toate tabelele trebuie să asigure integritatea datelor prin utilizarea obligatorie a cheilor primare şi, eventual, Foriegn Key.

6.3. Administrarea tehnică

Administrarea tehnică trebuie să asigure următoarele cerinţe:

- administrarea conturilor personale ale utilizatorilor din sistem (creare, modificare, suspendare, blocare, lichidare),
- implementarea politicii de securitate informațională;
- administrarea rolurilor (grupelor de utilizatori), gestionarea drepturilor de acces la sistem;
- vizualizarea şi analiza log-urilor din sistem (de aplicaţie, de sistem, web-server, baza de date etc.);
- administratorul tehnic nu va acces la informaţia din sistem prin aceste funcţii, nici prin acces direct;
- drepturile de administrator de sistem (aplicaţia, web-serwer, baza de date şi sistemul operaţional) nu sunt necesare pentru administrarea tehnică a SIA RSA;
- implementarea mecanismului de prelucrare a excepţiilor şi înştiinţare a administratorului tehnic despre apariția unor probleme pe diferite căi (poșta electronică, telefonul mobil ș.a.);
- asigurarea mecanismului copiilor de securitate şi a restabilirii informaţiei.

6.4. Managementul securității informaționale

Compania câștigătoare a concursului va elabora și implementa un sistem de management al securității informaționale conform exigențelor standardelor interaționale din clasa ISO 27000 și HG 1123. Va fi elaborat setul necesar de documente aferente securității informaționale. Vor fi instruite minimum 10 persoane responsabile de securitatea informațională.

Se va lua în considerație că accesul la baza de date a RSA trebuie permis pe niveluri de securitate stabilite conform legii. Persoanele care au acces la RSA pentru introducerea datelor sau pentru consultare vor fi desemnate prin dispoziție a MAI, respectiv prin dispoziție a persoanei responsabile din cadrul comisariatelor municipale/raionale în cazul structurile teritoriale de profil de la nivelul raioanelor sau al municipiilor.

Datele obținute în urma interogării sistemului vor fi utilizate în sensul și în limitele stabilite prin aprobarea acordată de conducerea structurilor abilitate.

Pentru prevenirea pierderilor accidentale ale datelor stocate în RSA va fi constituită Arhiva electronică a RSA, care va fi administrată de posesor/deținător. Arhiva electronică se va actualiza periodic conform cadrului tehnologic, pe baza datelor puse la dispoziție de persoanele desemnate din cadrul structurii abilitate.

Evidențele privind armele și munițiile letale și neletale constituie informații secrete, în conformitate cu prevederile Legii nr. 110-XIII din 18 mai 1994 cu privire la arme. Sistemul va asigura caracterul permanent al actualizării și păstrării datelor din evidențele RSA.

6.5. Fiabilitatea sistemului

SIA RSA trebuie să asigure funcţionalitatea corectă în regim de 24/7/365. Aceste cerinţe pot fi realizate prin utilizarea tehnologiilor de High Availability. Elaboratorul are dreptul de a implementa una din următoarele concepţii: Hot Standby sau Load Balancing. Aceste cerinţe sînt aplicabile pentru toate elementele sistemului.

În acelaşi timp, elaboratorul trebuie să asigure mecanisme şi proceduri de Backup şi Recovery. Backup-urile trebuie implementate în mod regulat, preferabil după schema GFS (grandfather – father – son, zilnic, săptămînal, lunar). Se recomandă utilizarea backup-urilor complete şi incrementale. Păstrarea copiilor este necesar de efectuat pe suport electronic în afara sistemului.

Pentru optimizarea procesului de backup, copiile de securitate trebuie organizate în regim de operaţiuni programate (pe perioada sarcinii minime a sistemului), precum şi manual, la iniţiativa Administratorului.

Elaboratorul este de asemenea obligat să asigure instrucţiuni clare referitor la restabilirea şi relansarea SIA RSA în regim de urgenţă, precum şi limitarea sarcinii maxime în cazuri de utilizare în aceste situaţii. În acelaşi timp, sistemul trebuie să fie asigurat cu un sistem de monitorizare a performanţelor principale şi un mecanism de alarmă în cazul depăşirii parametrilor predefiniți sau utilizării excesive de către utilizatorii de sistem cu notificarea Administratorului.

7. Testarea şi primirea

Primirea sistemului va fi permisă numai în cazul trecerii cu succes a testelor. Elaboratorul este responsabil pentru asigurarea testării. Aceste responsabilităţi includ:

- testarea funcţională;
- testarea sub sarcină.

La testarea funcţională este necesară demonstrarea corespunderii generale a sistemului elaborat în raport cu Sarcina Tehnică. Se va verifica corectitudinea și completitudinea implementării funcțiilor sistemului conform Sarcinii Tehnice, tipurilor şi valorilor limită ale datelor de intrare, comoditatea utilizării produsului software şi aspectul prietenos al interfeţei pentru utilizator.

La testarea sub sarcina se va verifica comportamentul sistemului la sarcini mai mari decît valorile maxime ale procesului de exploatare. În acest caz se va analiza şi documenta nivelul de performanţă al componentelor hardware (CPU usage, memory usage, network bandwidth, etc.) şi a timpului de răspuns al sistemului. Sistemul trebuie să asigure performanţe satisfăcătoare la sarcini care întrec valorile maxime preconizate (valori, care vor fi concretizate în Sarcina Tehnică) de cel puţin 10 ori.

La efectuarea testărilor toate erorile şi observaţiile detectate vor fi documentate în comun de Elaborator şi Beneficiar. În procesele verbale erorile vor fi clasificate în următoarele grupe:

- critice, care au cauzat stoparea procesului tehnologic sau au provocat deranjamente în funcţionarea programului;
- moderate, care cauzează incomoditate în lucru sau care au influenţă negativă asupra productivităţii sau securităţii sistemului, inclusiv limitează funcţionalitatea sistemului;
- erori ale procesului de proiectare, care solicită extinderea/modificarea funcţionalităţilor sistemului, care ies din limitele Sarcinii Tehnice.

În acelaşi timp se va verifica documentaţia prezentată privind conţinutul şi calitatea executării, analiza tehnologiilor aplicate, algoritmilor şi codului de program, precum şi realizarea cerinţelor.

Primirea sistemului se organizează prin exploatarea experimentală. După înlăturarea erorilor critice sistemul trece repetat testarea de calificare. Exploatarea experimentală se admite după înlăturarea tuturor erorilor din această grupă. Erorile moderate se înlătură în timpul exploatării experimentale.

Erorile procesului de proiectare vor fi analizate de către Elaborator în comun cu Beneficiarul. La fiecare din ele se vor lua decizii separate, în baza cărora vor fi perfectate procese-verbal.

Primirea sistemului se face în baza unui proces-verbal cu condiţia obligatorie de înlăturare a tuturor erorilor depistate şi exploatarea experimentală timp de două luni în care nu vor apărea observaţii, legate de noi erori.

Toate drepturile de autor vor fi transmise PNUD Moldova.

8. Cerinţe finale

8.1. Documentația

Toate documentele vor fi elaborate în limba română şi rusă. La realizarea sistemului este obligatorie elaborarea următoarelor documente:

- Ghidul utilizatorului;
- Ghidul administratorului;
- Ghidul programatorului;
- Setul de documente referitor la managementul securităţii informaţionale.

Ghidul utilizatorului trebuie să conţină informaţia generală despre sistem şi instrucţiuni clare şi accesibile privind utilizarea sistemului (intrare/ieşire din sistem). Aceste instrucţiuni vor fi elaborate pentru fiecare din business-rolurile din sistem şi procesele respective.

Ghidul administratorului trebuie să conţină informaţia detaliată despre arhitectura RSA, proceduri clare, accesibile şi succinte privind instalarea sistemului şi/sau modulelor respective, administrarea utilizatorilor şi drepturilor lor în sistem, deservirea sistemului, executarea copiilor de rezervă şi restabilire a sistemului, monitorizarea performanţelor şi a accesului.

Ghidul programatorului reflectă modul în care a fost elaborat acest sistemul, descrierea detaliată a arhitecturii, tehnologiilor şi instrumentelor utilizate (interpretoare, compilatoare, medii integrate de dezvoltare a softului, versiuni, modul de licenţiere), explicarea clară şi succintă a structurii bazelor de date, proceselor şi fluxurilor informaţionale, relaţiilor între diferite obiecte, codul modulelor, funcţiilor şi procedurilor cu indicaţia parametrilor de intrare şi ieşire, prelucrarea excepţiilor şi algoritmilor corespunzători.

8.2. Produse la ieșire

În cadrul acestui proiect aplicantul urmează să ofere următoarele produse şi servicii:

- Softul sistemului informatic „Registrul de Stat al Armelor”;
- Documentaţia în versiune electronică prezentată pe CD;
- Raportul rezultatelor testării interne;
- Instalarea softului pe serverul Beneficiarului în baza surselor prezentate pe CD;
- Instruirea şi consultarea utilizatorilor şi a personalului tehnic (50-60 persoane) la sediul elaboratorului sau în încăperi închiriate de către acesta, dotate special cu tehnică pentru petrecerea activităților de instruire;
- Implementarea sistemului în cadrul Ministerului Afacerilor Interne;
- Deservirea totală a sistemului, oferirea de consultanţă şi eliminarea erorilor pe durata a trei ani calendaristici.

8.3. Etapele realizării sarcinilor

Etapa I – 8 săptămâni

După semnarea contractului va fi elaborată, coordonată şi aprobată Sarcina Tehnică. Paralel va fi realizat designul sistemului, modelarea datelor, designul interfeţei, planul de testări şi de calitate. Documentul cu privire la designul tehnic al sistemului va fi prezentat, coordonat şi aprobat de Grupul de lucru al MAI și PNUD.

Etapa II – 8 săptămâni

În cadrul acestei etape va fi elaborat sistemul şi realizată testarea funcțională și sub sarcină. Va fi elaborată, coordonată şi aprobată documentaţia şi rezultatele testărilor de către MAI.

Etapa III – 4 săptămâni

În cadrul acestei etape va fi realizat planul de implementare.

Etapa IV – 4 săptămâni

Va include monitorizarea post-instalare şi corectarea erorilor. În caz de necesitate vor fi introduse modificîri în produsul program şi documentaţie. Va fi semnat Quality Review Document cu MAI.

Etapa V – 2 săptămâni

Va fi realizat cursul de instruire pentru administratori, programatori și utilizatori. La această etapă va fi semnat procesul verbal de predare-primire a lucrărilor după care vor fi prezentate şi acceptate toate produsele de la p. 8.2.

Etapa VI – 36 luni calendaristice

Va fi oferit serviciul de deservire totală a sistemului cu înlăturarea erorilor. În cadrul acestei etape va fi oferită consultanţă prin telefon la solicitare şi prin vizite la beneficiar.

Etapele I – V vor avea intervale de execuție paralelă în așa mod încât durata totală a proiectului să nu depășească 4 luni calendaristice.