IEPIRKUMA NOLIKUMS

(saskaņā ar Publisko iepirkumu likuma 9.panta ceturto daļu)

1. **Informācija par pasūtītāju**: Sabiedrisko pakalpojumu regulēšanas komisija
2. **Reģistrācijas numurs**: 90001162258
3. **Adrese**: Ūnijas iela 45, Rīga, LV-1039
4. **Tālr.**: 67097200, **Fakss**: 67097277
5. **E-pasta adrese**: sprk@sprk.gov.lv
6. **Mājas lapa**: www.sprk.gov.lv
7. **Pasūtītāja kontaktpersonas**:

   7.1. Pasūtītāja kontaktpersona ar piedāvājumu iesniegšanu saistītos jautājumos: Administratīvā departamenta Tehniskā nodrošinājuma nodaļas vadītāja p.i. Artis Zverovs, tālrunis: 67097257, e-pasta adrese:**artis.zverovs@sprk.gov.lv**;

   7.2. Pasūtītāja kontaktpersona ar tehnisko specifikāciju saistītos jautājumos: - Informācijas sistēmu departamenta direktora p.i. Didzis Šapkus, tālrunis 67873856, e-pasta adrese: **didzis.sapkus@sprk.gov.lv**
8. **Iepirkuma identifikācijas numurs**: SPRK 2017/260
9. **Iepirkuma līguma veids**:

Būvdarbi	
Piegāde	
Pakalpojumi	X

10. **Iepirkuma priekšmets un apjoms:** Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana (turpmāk – IT drošības audits)
11. **CPV kods**: 72810000-1 "Datoru audita pakalpojumi"; 72150000-1 "Datoru audita konsultāciju un datortehnikas konsultāciju pakalpojumi"; 72220000-3 "Sistēmu un tehnisko konsultāciju pakalpojumi."
12. **Paredzamā līgumcena (bez PVN):** līdz 20 660,00 EUR (divdesmit tūkstoši seši simti sešdesmit *euro* un 0 centi)
13. **Iepirkuma līguma izpildes vieta**: Rīgā, Ūnijas ielā 45.
14. **Iepirkuma līguma izpildes termiņš**: 3 (trīs) mēneši no līguma noslēgšanas dienas.
15. **Pretendents var iesniegt piedāvājumus:**

par daļu no apjoma	
par vairākām daļām	
tikai par visu apjomu	X

16. **Pretendents var iesniegt vairākus piedāvājuma variantus:**

Jā	
Nē	X

17. **Minimālās prasības attiecībā uz piedāvājuma variantiem un specifiskās prasības variantu iesniegšanai:** nav

18. Pretendents piedāvājuma variantus var iesniegt tikai tad, ja ir iesniegts arī piedāvājums, kas nav variants:

Jā	
Nē	X

19. Pretendentam jāiesniedz:

19.1. Dokumenta kopija, kas apliecina, ka pretendents ir reģistrēts NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī (2015.gada 28.jūlija Ministru kabineta noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 36.punkts);

19.2. Pretendenta apliecinājums, ka tā darbinieki, kas tiks iesaistīti IT drošības audita veikšanā ir NATO, Eiropas Savienības, Eiropas Ekonomiskās zonas valstu pilsoņi vai Latvijas Republikas nepilsoņi un pretendents apstrādās IT drošības audita laikā iegūto informāciju vienīgi NATO, Eiropas Savienības un Eiropas Ekonomiskās zonas valstu teritorijā (2015.gada 28.jūlija Ministru kabineta noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 35.punkts);

19.3. Rakstisks pieteikums dalībai iepirkumā (pielikums Nr.1);

19.4. Tehniskais piedāvājums (pielikums Nr.2) atbilstoši Tehniskās specifikācijas (pielikums Nr.3) prasībām.

19.5. Finanšu piedāvājums (pielikums Nr.4) noteiktajām prasībām.

19.6. Informācija par pretendenta pieredzi par vismaz 2 (diviem) pasūtījumiem, kur IT drošības audits veikts informācijas sistēmai, kuras izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro,* 0 centi) un, kas apstrādā fizisko personu datus, un IT drošības audits ticis veikts saskaņā ar OWASP (Open Web Application Security Project) un OSSTMM (Open Source Security Testing Methodology Manual) vai līdzvērtīgiem standartiem; veikta IT drošības audita un veiktspējas testēšana, kur vismaz 1 (vienas) informācijas sistēmas izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro*, 0 centi) un IT drošības pārvaldības audits veikts atbilstoši ISO/IEC 27001:2013 standarta prasībām informācijas sistēmai, kuras izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro,* 0 centi):

19.6.1. norādot pakalpojuma saņēmēja nosaukumu;

19.6.2. norādot īsu pakalpojuma aprakstu;

19.6.3. norādot pakalpojuma īstenošanas laiku;

19.6.4. norādot pakalpojuma finanšu apmēru;

19.6.5. norādot pasūtītāja kontaktpersonu (vārds uzvārds, amats, tālruņa numurs, e-pasta adrese);

19.6.6. pievienojot vismaz 2 (divas) klientu atsauksmes.

19.7. Pretendenta plānotais līguma izpildes kalendārais grafiks saskaņā ar Iepirkuma nolikuma tehniskajā specifikācijā noteikto formu par katru IT drošības audita darbu norādot:

19.7.1. konkrēto IT drošības audita darbu atbilstoši Finanšu piedāvājuma tabulā norādītajiem IT drošības audita darbiem;

19.7.2. kalendāro dienu skaitu, kas nepieciešams, lai iepazītos ar sistēmu vai IT infrastruktūras komponentēm konkrētā IT drošības audita darba veikšanai;

19.7.3. IT drošības audita darba plānoto izpildes termiņu (kalendārās dienas);

19.7.4. informāciju vai konkrēto IT drošības audita darbu plānots veikt paralēli citam šī IT drošības audita ietvaros veicamajam IT drošības audita darbam (ja jā, tad paralēli kuram);

19.7.5. kalendāro dienu skaitu, kas nepieciešams ziņojuma iesniegšanai par konkrēto IT drošības audita darbu;

19.7.6. konkrētā IT drošības audita darba kopējo izpildes laiku (kalendārās dienas);

19.7.7. kalendāro dienu skaitu, kas nepieciešams IT drošības audita gala ziņojuma iesniegšanai par visiem IT drošības audita darbiem.

19.8. Pretendenta izziņa, ka pretendenta vidējais finanšu apgrozījums iepriekšējos 3 (trīs) pārskata gados (2014, 2015, 2016), vai visu darbības periodu, ja pretendenta faktiskais darbības laiks ir mazāks, iepirkuma priekšmetam līdzvērtīgu pakalpojumu jomā ir vismaz 30 000 *euro* (trīsdesmit tūkstoši *euro*) bez PVN.

19.9. Pretendenta informācija par piedāvāto darba grupas sastāvu, pievienojot speciālistu pašrocīgi parakstītus CV (atbilstoši Iepirkuma nolikuma tehniskajā specifikācijā noteiktajai formai) ar informāciju par nepieciešamo kvalifikāciju un pieredzi, sertifikātu un izglītību apliecinošo dokumentu kopijas atbilstoši Iepirkuma nolikuma 22.punktā noteiktajām prasībām.

20. Pretendenta izslēgšanas nosacījumi: Pasūtītājs pretendentu, kuram būtu piešķiramas iepirkuma līguma slēgšanas tiesības, izslēdz no turpmākas dalības Iepirkumā pamatojoties uz Publisko iepirkumu likuma 9.panta astotajā daļā noteiktajiem gadījumiem.

21. Informācijas aizsardzības noteikumi, ja tādi nepieciešami, ņemot vērā Publisko iepirkumu likuma 14.panta pirmo daļu:

21.1. informācija (materiālā un nemateriālā formā), ko pretendents vai pretendenta darbinieki tīši vai netīši iegūs IT drošības audita izpildes laikā, ir uzskatāma par ierobežotas pieejamības informāciju, un tās izpaušana trešajām personām bez Pasūtītāja rakstiskas piekrišanas ir aizliegta;

21.2. pirms piedāvājuma iesniegšanas pretendents ir iepazinies ar Latvijas likumu un citu tiesību aktu normām par ierobežotas pieejamības informāciju, komercnoslēpumu, par informāciju, kurai normatīvajos aktos paredzēta īpaša izmantošanas kārtība un izplatīšanas liegums, kā arī personu vai institūciju loku, kurām tiesību aktos ir noteiktas tiesības šādu informāciju pieprasīt vai saņemt;

21.3. pretendentam ir pienākums nodrošināt, ka tā amatpersonas, darbinieki, konsultanti un citas personas, kuras izmantos Pasūtītāja informāciju, saņems un izmantos to vienīgi Iepirkuma līguma izpildes nodrošināšanai un tikai nepieciešamajā apjomā;

21.4. pretendents ar sava piedāvājuma iesniegšanu apliecina, ka viņš saprot un apzinās, ka konfidencialitātes noteikumi ir saistoši arī pēc Iepirkuma līguma termiņa beigām, kā arī pēc pirmstermiņa līgumattiecību izbeigšanas;

21.5. ja informācijas, kuru pretendentam sniedz Pasūtītājs IT drošības audita laikā, izpaušanas rezultātā Pasūtītājam vai trešajām personām tiks nodarīti tieši zaudējumi, vai pretendents izmantojis informāciju iedzīvošanās nolūkā vai to izpaudis par maksu, viņš mantiski atbildēs tiesību aktos noteiktā kārtībā un apmērā.

22. Prasības pretendenta profesionālajām spējām: pretendentam jānodroša šādu speciālistu piesaisti IT drošības audita realizācijā, ievērojot nosacījumu, ka viens piedāvātais speciālists nedrīkst piedalīties IT drošības auditā vairāk kā divās lomās. Piedāvātajiem speciālistiem ir jāspēj komunicēt latviešu valodā vai arī pretendentam ir jānodrošina tulks. Pierādot piedāvātā speciālista kvalifikāciju par pieredzi projektos, aizpildot par katru piedāvāto speciālistu pieredzes aprakstu (CV) atbilstoši Iepirkuma nolikuma tehniskajā specifikācijā noteiktajai formai un jāiesniedz speciālistu apmācību pamatojošo dokumentu un sertifikātu kopijas:

22.1. **projektu vadītājs - informācijas drošības eksperts**, kuram ir:

22.1.1. augstākā izglītība informāciju tehnoloģiju drošībā **vai** augstākā izglītība vadības zinībās vai informācijas tehnoloģijās un sertifikāts, kas apliecina projekta vadītāja zināšanas (PMP vai IPMA sertifikāts vai ekvivalents), sertifikāts, kas apliecina zināšanas kā informācijas sistēmu auditoram (CISA vai ekvivalents), sertifikāts, kas apliecina zināšanas drošības pārvaldībā un ISO 27001 audita veikšanā (ISO 27001 Lead auditor sertifikāts vai ekvivalents);

22.1.2. pieredze iepriekšējo 3 (trīs) gadu laikā (līdz piedāvājuma iesniegšanas termiņa beigām) kā projektu vadītājam vismaz 1 (vienā) informāciju tehnoloģiju drošības audita un veiktspējas pakalpojuma sniegšanā informācijas sistēmai, kuras izstrādes finanšu apjoms ir vismaz 100 000 *euro* (simts tūkstoši *euro*, 0 centi).

22.2. **Vadošais informācijas sistēmu drošības speciālists - auditors**, kuram ir:

22.2.1. augstākā izglītība informāciju tehnoloģiju drošībā **vai** augstākā izglītība vadības zinībās vai informācijas tehnoloģijās, sertifikāts, kas apliecina zināšanas drošības pārvaldības tehniskajos jautājumos (CISSP vai ekvivalents), sertifikāts, kas apliecina zināšanas kā informācijas sistēmu auditoram (CISA vai ekvivalents);

22.2.2. praktiska pieredze IT jomā un veicis IT drošības auditu informācijas sistēmai, kuras izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro,* 0 centi);

22.3. **Informācijas drošības ielaušanās speciālists**, kuram ir:

22.3.1. augstākā izglītība informāciju tehnoloģiju drošības jomā **vai** augstākā izglītība vadības zinībās vai informācijas tehnoloģijās, sertifikāts, kas apliecina zināšanas kā informācijas drošības ielaušanās speciālistam (CEH vai GPEN, vai ekvivalents);

22.3.2. praktiska pieredze IT jomā, kurš veicis informācijas drošības ielaušanās testus informācijas sistēmai, kuras izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro,* 0 centi) un IT drošības audits veikts, izmantojot OWASP, OSSTMM metodoloģiju;

22.4. **Informāciju sistēmu veiktspējas testēšanas speciālists**, kuram ir:

22.4.1. augstākā izglītība vadības zinībās vai informācijas tehnoloģijās;

22.4.2. sertifikāts, kas apliecina zināšanas informācijas sistēmu testēšanā (ISTQB vai ekvivalents);

22.4.3. praktiska pieredze IT jomā un, kurš veicis veiktspējas testēšanu informācijas sistēmai, kuras izstrādes cena ir vismaz 100 000 *euro* (viens simts tūkstoši *euro,* 0 centi). Gadījumā, ja tiek piedāvāts atvērtā pirmkoda produkts, speciālistam jābūt ar dokumentētu pieredzi vismaz 1 (viena) veiktspējas testēšanas projektā izmantojot atvērtā pirmkoda produktu iepriekšējo 3 (trīs) gadu laikā;

22.5. **Fizisko personu datu aizsardzības speciālists**, kurš, atbilstoši Fizisko personu datu aizsardzības likumam, ir ieguvis personas datu aizsardzības speciālista statusu (apliecinājums – Datu valsts inspekcijas izdots derīgs sertifikāts).

23. Prasības piedāvājumu noformējumam un saturam:

23.1. **Piedāvājumi jāiesniedz**: Sabiedrisko pakalpojumu regulēšanas komisijai Ūnijas ielā 45, Rīgā, LV-1039, slēgtā aploksnē vienā eksemplārā līdz 2017.gada 9.oktobrim, plkst.12:00. Piedāvājumi jāiesniedz personīgi vai nosūtot pa pastu ierakstītā vēstulē. Pasta sūtījumam jābūt nogādātam šajā punktā norādītajā adresē līdz šajā punktā noteiktajam termiņam. Piedāvājumi, kas iesniegti pēc minētā termiņa, tiek izslēgti no dalības iepirkumā.

23.2. **uz piedāvājuma aploksnes jānorāda**:

23.2.1. pretendents (nosaukums, reģistrācijas numurs un juridiskā adrese);

23.2.2. iepirkuma identifikācijas numurs;

23.2.3. iepirkuma nosaukums;

23.2.4. norāde "Neatvērt līdz 2017.gada 9.oktobrim, plkst. 12:00".

23.3. ja pretendents iesniedz dokumentu kopijas vai norakstus, dokumenta kopija vai noraksts jāapliecina LR normatīvajos aktos noteiktajā kārtībā, proti – atbilstoši Ministru kabineta 2010.gada 28.septembra noteikumu Nr.916 „Dokumentu izstrādāšanas un noformēšanas kārtība" prasībām. Svešvalodās pievienotiem dokumentiem jābūt tulkotiem LR valsts valodā;

23.4. ja piedāvājumu ir parakstījusi persona, kurai saskaņā ar pretendenta statūtiem nav noteiktas paraksta tiesības, piedāvājumam jāpievieno pilnvara.

23.5. pēc piedāvājuma iesniegšanas termiņa beigām pretendents nevar savu piedāvājumu grozīt.

24. Piedāvājumu vērtēšana un izvēles kritēriji:

24.1. pretendenta piedāvājuma atbilstības Iepirkuma nolikumam vērtēšanu Iepirkumu komisija veic slēgtā sēdē bez pretendenta klātbūtnes;

24.2.Iepirkumu komisija var neizskatīt pretendenta piedāvājumu un noraida vai izslēdz pretendentu no turpmākās dalības iepirkumā, ja:

24.2.1. pretendents, iesniedzot pieprasīto informāciju, norādījis nepatiesas ziņas;

24.2.2. pretendents vispār nav sniedzis ziņas;

24.2.3. piedāvājuma dokumenti nav iesniegti atbilstoši noteiktajām prasībām un dokumenta neatbilstība ir būtiska pretendenta piedāvājuma izvērtēšana;

24.2.4. pretendents ir izslēdzams no dalības iepirkumā saskaņā ar Publisko iepirkumu likuma 9.panta astoto daļu;

24.3. saimnieciski visizdevīgākā piedāvājuma kritērijs šī iepirkuma ietvaros ir zemākā cena.

24.4. par uzvarētāju tiek atzīts pretendents, kurš iesniedzis atbilstoši Iepirkuma nolikumā noteiktajām prasībām noformētu piedāvājumu, nav noraidāms vai izslēdzams no dalības iepirkumā saskaņā ar Publisko iepirkumu likuma 9.panta astoto daļu, un finanšu piedāvājumā piedāvājis saimnieciski visizdevīgāko piedāvājumu zemāko cenu.

25. Iepirkuma rezultātu paziņošana:

Pasūtītājs 3 (trīs) darbdienu laikā pēc lēmuma pieņemšanas informē visus pretendentus par iepirkumā izraudzīto pretendentu, nosūtot rakstveida paziņojumu pretendentiem un izvietojot lēmumu Sabiedrisko pakalpojumu regulēšanas komisija mājas lapā internetā: www.sprk.gov.lv.

26. Iepirkuma līguma slēgšanas kārtība:

26.1. Iepirkuma līgumu slēdz ne ātrāk kā nākamajā dienā pēc Publisko iepirkumu likuma 9.panta četrpadsmitajā daļā minētā paziņojuma nosūtīšanas dienas, bet ne vēlāk kā līdz pēdējai pretendenta piedāvājuma derīguma termiņa dienai;

26.2. Pretendentam ir tiesības uzdot jautājumus par Iepirkuma nolikumā ietvertajām prasībām, t.sk. par iepirkuma līguma projektu Publisko iepirkumu likuma 9.panta sestajā daļā noteiktajos termiņos;

26.3. Ja pretendents, kuram piešķirtas iepirkuma līguma slēgšanas tiesības, atsakās slēgt iepirkuma līgumu ar Pasūtītāju, Iepirkumu komisija ir tiesīga pieņemt lēmumu iepirkuma līguma slēgšanas tiesības piešķirt nākamajam pretendentam, kurš piedāvājis saimnieciski visizdevīgāko piedāvājumu, vai izbeigt iepirkuma procedūru bez rezultāta. Ja pieņemts lēmums iepirkuma līguma slēgšanas tiesības piešķirt nākamajam pretendentam, kurš piedāvājis saimnieciski visizdevīgāko piedāvājumu, bet tas atsakās slēgt iepirkuma līgumu, Iepirkumu komisija pieņem lēmumu pārtraukt iepirkuma procedūru, neizvēloties nevienu piedāvājumu.

27. Piedāvājuma derīguma termiņš:

Piedāvājumam jābūt spēkā vismaz 45 (četrdesmit piecas) dienas no piedāvājumu iesniegšanas dienas, bet iepirkuma uzvarētājam - līdz līgumsaistību pilnīgai izpildei.

28. Iepirkuma priekšmeta tehniskā specifikācija: pielikums Nr.3

29. Prasības iepirkuma finanšu piedāvājumam:

29.1. Finanšu piedāvājums jāsagatavo saskaņā ar pievienoto finanšu piedāvājuma veidlapu (pielikums Nr.4);

29.2. Finanšu piedāvājumam jābūt izteiktam euro (EUR), atsevišķi norādot piedāvājuma summu ar un bez PVN, kā arī kopējo summu;

29.3. Finanšu piedāvājuma summā jāiekļauj visas tiešās, pieskaitāmās izmaksas, kā arī neparedzētie izdevumi, ja tādi var rasties iepirkuma līguma izpildes laikā.

Iepirkumu komisijas priekšsēdētāja _____ **/D.Jansone/**

Pielikums Nr.1
Iepirkumam Nr. SPRK 2017/260

Pretendenta pieteikums dalībai iepirkumā Nr. 2017/260 "Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana "

Saskaņā ar Iepirkuma nolikumu, es, apakšā parakstījies, apliecinu, ka:

1. *<Pretendenta nosaukums>* (turpmāk – pretendents) piesakās dalībai iepirkumā un piekrīt Iepirkuma nolikumā un tā pielikumos noteiktajam un garantē iepirkuma prasību pilnīgu izpildi. Iepirkuma nolikumā ietvertās prasības ir skaidras un saprotamas;
2. visas piedāvājumā sniegtās ziņas par pretendentu un piedāvāto pakalpojumu ir patiesas;
3. pretendentam ir pietiekami finanšu, personāla un tehniskie resursi pakalpojuma sniegšanai;
4. pretendenta piedāvājums ir spēkā 45 (četrdesmit piecas) dienas no noteiktā piedāvājumu iesniegšanas termiņa un var tikt akceptēts jebkurā laikā pirms tā spēkā esamības termiņa beigām;
5. ar piedāvājuma izteikšanu piedalīties iepirkumā pretendents uzņemas pienākumu neizpaust vai kā citādi izmantot iepirkuma ietvaros iegūto informāciju.
6. piekrītu / nepiekrītu izmantot drošu elektronisko parakstu saziņā ar pasūtītāju.
   (nevajadzīgo svītrot)

Pretendenta nosaukums: _____

Reģistrēts (vieta, datums): _____

Nodokļu maksātāja reģ. Nr.: _____

Juridiskā adrese: _____

Pretendenta telefona Nr.: _____

Pretendenta fakss: _____

Pretendenta e-pasta adrese: _____

Pretendenta interneta vietnes adrese: _____

Kredītiestādes rekvizīti: _____

Kontaktpersona: (Vārds, uzvārds, amats) _____

Kontaktpersonas telefons: _____

Kontaktpersonas e-pasta adrese: _____

Pieteikuma aizpildīšanas datums: _____

Vadītāja vai pilnvarotās personas paraksts:	
Vārds, uzvārds:	
Amats:	

Iepirkumu komisijas priekšsēdētāja _____ **/D.Jansone/**

Pielikums Nr.2
Iepirkumam Nr. SPRK 2017/260

TEHNISKAIS PIEDĀVĀJUMS
iepirkumam Nr. 2017/260
"Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana "

Pretendents Tehnisko piedāvājumu sagatavo saskaņā ar Tehniskajā specifikācijā noteiktajām prasībām, iesniedzot detalizētu aprakstu par iepirkuma priekšmetu atbilstoši šādai formai:

Nr.p.k.	IT drošības audita darba apjoms	Detalizēts apraksts
1.	**Informācijas drošības novērtējums atbilstoši ISO/IEC 27001:2013 standarta kontrolēm**	
1.1.	IT drošības audita darba izpildes apraksts	
1.2.	Identificētais IT drošības audita darba saturs	
1.3.	Paredzamais IT drošības audita darba rezultāts	
1.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
1.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
2.	**Sociālās inženierijas testi un drošības novērtējums**	
2.1.	IT drošības audita darba izpildes apraksts	
2.2.	Identificētais IT drošības audita darba saturs	
2.3.	Paredzamais IT drošības audita darba rezultāts	
2.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
2.5.	Sagatavojamie un Pasūtītājam iesniedzamie	

	nodevumi	
3.	**Lietotāju darbstaciju satura pārbaudes**	
3.1.	IT drošības audita darba izpildes apraksts	
3.2.	Identificētais IT drošības audita darba saturs	
3.3.	Paredzamais IT drošības audita darba rezultāts	
3.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
3.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
4.	**Fiziskās drošības novērtēšana**	
4.1.	IT drošības audita darba izpildes apraksts	
4.2.	Identificētais IT drošības audita darba saturs	
4.3.	Paredzamais IT drošības audita darba rezultāts	
4.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
4.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
5.	**Drošības, veiktspējas un pieejamības novērtēšana Komersantu informācijas ievades un apstrādes sistēmai (IIAS)**	
5.1.	IT drošības audita darba izpildes apraksts	
5.2.	Identificētais IT drošības audita darba saturs	
5.3.	Paredzamais IT drošības audita darba rezultāts	

5.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
5.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
6.	**Drošības, veiktspējas un pieejamības novērtēšana Starpsavienojumu datu bāzei (STARS)**	
6.1.	IT drošības audita darba izpildes apraksts	
6.2.	Identificētais IT drošības audita darba saturs	
6.3.	Paredzamais IT drošības audita darba rezultāts	
6.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
6.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
7.	**Drošības, veiktspējas un pieejamības novērtēšana Elektroniskai dokumentu uzskaites sistēmai (EDUS)**	
7.1.	IT drošības audita darba izpildes apraksts	
7.2.	Identificētais IT drošības audita darba saturs	
7.3.	Paredzamais IT drošības audita darba rezultāts	
7.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
7.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
8.	**Drošības, veiktspējas un pieejamības novērtēšana grāmatvedības un peronālvadības sistēmai (Ozols)**	

8.1.	IT drošības audita darba izpildes apraksts	
8.2.	Identificētais IT drošības audita darba saturs	
8.3.	Paredzamais IT drošības audita darba rezultāts	
8.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
8.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
9.	**Drošības, veiktspējas un pieejamības novērtēšana Sabiedrisko pakalpojumu regulēšanas komisijas failu glabātuves sistēmai**	
9.1.	IT drošības audita darba izpildes apraksts	
9.2.	Identificētais IT drošības audita darba saturs	
9.3.	Paredzamais IT drošības audita darba rezultāts	
9.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	
9.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	
10.	**Kopējo IT infrastruktūras komponenšu drošības novērtēšana**	
10.1.	IT drošības audita darba izpildes apraksts	
10.2.	Identificētais IT drošības audita darba saturs	
10.3.	Paredzamais IT drošības audita darba rezultāts	
10.4.	Kritēriji IT drošības audita darba un tā rezultāta akceptēšanai	

10.5.	Sagatavojamie un Pasūtītājam iesniedzamie nodevumi	

Vadītāja vai pilnvarotās personas paraksts:	
Vārds, uzvārds:	
Amats:	

Iepirkumu komisijas priekšsēdētāja /D.Jansone/

Pielikums Nr.3
Iepirkumam Nr. SPRK 2017/260

TEHNISKĀ SPECIFIKĀCIJA
iepirkumam Nr. SPRK 2017/260
"Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana"

I. Vispārējais apraksts

1. Sabiedrisko pakalpojumu regulēšanas komisijas (turpmāk - Regulators) informācijas sistēmas nodrošina Regulatora ikdienas darbu. IT drošības audita ietvaros ir jāveic Regulatora informācijas un informācijas sistēmu drošības pārbaudes atbilstoši šajā tehniskajā specifikācijā noteiktajām prasībām, kas ietver:

   1.1. informācijas drošības politikas un ar to saistošās dokumentācijas, un ārēju un iekšējo normatīvo dokumentu izvērtēšanu, atbilstoši LR normatīvajiem aktiem un IT jomu reglamentējošiem dokumentiem, tai skaitā ISO/IEC 27001:2013 standartam;

   1.2. tehnisko resursu fiziskās drošības pārbaudes un sociālās inženierijas testus un drošības novērtēšanu, kā arī Regulatora darbinieku darbstaciju satura pārbaudes (darbi tiek veikti attiecinot tos uz Regulatoru kopumā, nevis konkrētu informācijas sistēmu);

   1.3. informācijas sistēmu drošības, pieejamības un veiktspējas testēšanu un novērtēšanu;

   1.4. kopējo IT infrastruktūras komponenšu drošības novērtēšanu (darbi tiek veikti attiecinot tos uz Regulatoru kopumā, nevis konkrētu informācijas sistēmu).

II. Auditējamo sistēmu un IT infrastruktūras komponenšu apraksts

2. **Pamatdarbības informācijas sistēmas:**

   2.1. **IIAS jeb Komersanta informācijas ievades un apstrādes sistēma** ir Regulatora izstrādāta un pārziņā esoša sistēma, ar kuras starpniecību regulējamie sabiedrisko pakalpojumu sniedzēji (turpmāk – komersanti) Regulatoram elektroniski iesniedz normatīvajos aktos noteikto informāciju - atskaites un dokumentus. Sistēmas mērķis ir komersantu datu ievade, uzkrāšana, apstrāde un analīze, nodrošinot iespēju drošā veidā komersantiem iesniegt visas nepieciešamās veidlapas elektroniski un komunicēt ar Regulatoru, izmantojot sistēmā ievietotus ziņojumus;

   2.2. **STARS jeb Starpsavienojumu datu bāze** ir izstrādāta, lai uzkrātu informāciju par komersantu savstarpēji noslēgtajiem starpsavienojumu līgumiem un nodrošinātu to analīzi pēc dažādiem parametriem. Reģistrējamie dati ir: noslēgšanas datums, spēkā stāšanās datums, starpsavienojuma izveides parametri, starpsavienojuma savstarpējie tarifi u.c.;

   2.3. **EDUS jeb elektroniskās dokumentu uzskaites sistēmas** mērķis ir nodrošināt informācijas uzglabāšanu un apriti Regulatorā (dokumentu uzglabāšanu, sistematizēšanu, datu apkopošanu, dokumentu vizēšanu un parakstīšanu, informāciju par Regulatora darbinieku prombūtni u.c.);

   2.4. **OZOLS jeb grāmatvedības un personālvadības sistēma** nodrošina Regulatora finanšu un grāmatvedības informācijas uzskaiti, apstrādi un uzturēšanu, kā arī ar personāla vadību saistītas informācijas uzskaiti, uzturēšanu un apstrādi;

2.5. **Regulatora failu glabātuves sistēma** ir failu glabāšanas un pārvaldības serveris iekšējām Regulatora darbības nodrošināšanas vajadzībām;

2.6. **Kopējās IT infrastruktūras komponentes:**

2.6.1. Virtualizācijas vide;
2.6.2. Ugunsmūris;
2.6.3. Lokālais datortīkls (tai skaitā bezvadu tīkls);
2.6.4. Aktīvā direktorija.

III. IT drošības audita darbi drošības pārvaldības ietvaros

3. **Regulatora informācijas drošības novērtējums atbilstoši ISO/IEC 27001:2013 standartam:** IT drošības audita ietvaros jāveic kopējs Regulatora informācijas drošības novērtējums atbilstoši ISO/IEC 27001:2013 standarta kontrolēm.

4. **Sociālās inženierijas testi un drošības novērtējums:**

4.1. IT drošības audita ietvaros jāveic sociālās inženierijas testi, kā arī kopējais drošības novērtējums attiecībā uz sociālās inženierijas uzbrukumiem;

4.2. drošības novērtējums jābalsta uz attiecīgajām ISO/IEC 27001:2013 standarta kontrolēm un OSSTMM v3 drošības testēšanas rokasgrāmatas "Cilvēku drošības testēšanas" (*Human Security Testing)* kontrolēm.

5. **Lietotāju darbstaciju satura pārbaudes:**

5.1. IT drošības audita ietvaros jāveic Regulatora darbinieku darba vietu datoru (tai skaitā "*laptop*" datoru) satura pārbaudes attiecībā uz datoros instalēto programmatūru un datoros esošo informāciju – jānosaka, vai datoros ir uzstādīta lietojumprogrammatūra, kas nav nepieciešama Regulatora darbinieka pienākumu pildīšanai, un datoros neatrodas datnes un faili, kas ievietoti Regulatora darbinieku personiskām vajadzībām (piemēram, video formāta faili, kas satur izklaides materiālu);

5.2. par konkrētu pārbaudāmo programmatūru un informācijas uzglabāšanas failu jāvienojas ar Pasūtītāju pirms skenēšanas pārbaužu veikšanas.

6. **Fiziskās drošības novērtēšana:**

6.1. jāveic Regulatora informācijas tehnoloģiju tehnisko resursu fiziskās drošības novērtējums. Fiziskās drošības novērtējums ietver vismaz pārbaudes datu pārraides līniju piekļuvēm, datu centra vai serveru telpai un tās piekļuvei, klimata uzturēšanas iekārtām, elektrības nepārtrauktās barošanas elementiem;

6.2. fiziskās drošības novērtējums jābalsta uz attiecīgajām ISO/IEC 27001:2013 standarta kontrolēm.

IV. IT drošības audita darbi Regulatora informācijas sistēmu drošības un veiktspējas pārbaudei

7. **Sistēmas drošības novērtēšana:**

7.1. **Drošības novērtēšana atbilstoši LR un Regulatora iekšējiem normatīvajiem aktiem:**

7.1.1. **veicot sistēmas drošības novērtējumu, jāņem vērā šāds normatīvais regulējums:**

7.1.1.1. Informācijas tehnoloģiju drošības likums;

7.1.1.2. Fizisko personu datu aizsardzības likums;

7.1.1.3. Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām";

7.1.1.4. Regulatora iekšējie normatīvie akti;

7.1.1.5. citi IT jomu reglamentējoši normatīvie akti.

7.1.2. **Drošības novērtēšana atbilstoši ISO/IEC 27001:2013 standarta kontrolēm:**

7.1.2.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaude pret LVS ISO/IEC 27001:2013 standarta kontrolēm;

7.1.2.2. nav atkārtoti jāvērtē tās ISO/IEC 27001:2013 standarta kontroles, kuras jau pārbaudītas šī IT drošības audita ietvaros un ir attiecināmas uz visu Regulatoru kopumā (piemēram, Regulatora kopējās informācijas drošības politikas dokumenta izvērtēšana) un nav viennozīmīgi attiecināmas tikai uz konkrēto sistēmu.

7.1.3. **Drošības novērtēšana atbilstoši OSSTMM v3 drošības testēšanas rokasgrāmatai:**

7.1.3.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaudes testi pret katru no OSSTMM v3 (Open Source Security Testing Methodology Manual) rokasgrāmatas drošības testiem jeb prasībām. Pārbaudes jāveic atbilstoši OSSTMM v3 rokasgrāmatas "Bezvadu drošības testu" kontrolēm un "Datu tīkla drošības testu" kontrolēm;

7.1.3.2. nav atkārtoti jāvērtē tās OSSTMM v3 rokasgrāmatas kontroles, kuras jau pārbaudītas šī IT drošības audita ietvaros un ir attiecināmas uz visu Regulatoru kopumā (piemēram, Regulatora kopējās informācijas drošības politikas dokumenta izvērtēšana) un nav viennozīmīgi attiecināmas tikai uz konkrēto sistēmu.

7.1.4. **Drošības novērtēšana atbilstoši OWASP v4 "Testing guide" drošības testēšanas kontrolēm:**

7.1.4.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaudes testi pret katru no OWASP v4 (Open Web Application Security Project) *Testing guide* drošības testēšanas kontrolēm;

7.1.4.2. novērtējumam jāiekļauj pārbaudes par OWASP v4 Testing guide kontroļu grupām:

7.1.4.2.1. informācijas vākšana;
7.1.4.2.2. konfigurācijas pārvaldības testēšana;
7.1.4.2.3. identitātes pārvaldības testēšana;
7.1.4.2.4. autentifikācijas testēšana;
7.1.4.2.5. autorizācijas testēšana;
7.1.4.2.6. sesiju pārvaldības testēšana;
7.1.4.2.7. ievaddatu validācijas testēšana;
7.1.4.2.8. kļūdu apstrāde;
7.1.4.2.9. kriptogrāfija;
7.1.4.2.10. biznesa loģikas testēšana;
7.1.4.2.11. klienta puses testēšana.

7.1.5. **Sistēmas rezerves kopiju izveides un atjaunošanas procesa novērtēšana:**

7.1.5.1. IT drošības audita ietvaros jāveic sistēmas rezerves kopēšanas procesa un atjaunošanas plāna realizācija un pietiekamības novērtējums;

7.1.5.2. saskaņojot darbus ar Pasūtītāju, jāveic sistēmas rezerves kopijas sagatavošana un sistēmas darbības atjaunošana no iepriekš sagatavotās rezerves kopijas.

7.2. **Sistēmas veiktspējas un pieejamības novērtēšana:**

7.2.1. **Sistēmas stresa testi:**

7.2.1.1. sistēmas veiktspējas novērtēšanā jāveic informācijas sistēmas tehnisko resursu stresa testi un novērtējumi. Stresa testiem jāatspoguļo sistēmas tehnisko resursu noslodze atkarībā no vienlaicīgo sesiju (lietotāju) skaita. Stresa testu laikā atsevišķi ir jātestē informācijas sistēmas publiskā daļa (ja tāda ir), kā arī tā daļa, kas nav publiski pieejama, kopumā sniedzot vienotu skatu uz procesa norisi;

7.2.1.2. informācijas sistēmas stresa testu laikā plānotie iegūstamie tehnisko resursu noslodzes rādītāji ir iepriekš jāsaskaņo ar Pasūtītāju.

7.2.2. **Atteices DoS uzbrukuma testi:** sistēmas veiktspējas un pieejamības novērtēšanā jāveic DoS uzbrukumi, mēģinot iztukšot sistēmas, datu pārraides resursus vai izmantot informācijas apstrādes nepilnības.

7.2.3. **Testu veikšanas laiks:** informācijas sistēmas veiktspējas un pieejamības testi ir jāveic diennakts laikā no plkst.22:00 līdz plkst.7:00. Ja testējamo sistēmu darbības neietekmē sistēmu ekspluatāciju, tad, vienojoties ar Pasūtītāju, šos testus var veikt no plkst.7:00 līdz plkst.22:00.

7.2.4. **Sistēmas uzbūves analīze attiecībā uz veiktspēju un pieejamību:** sistēmas veiktspējas novērtēšanas laikā veicama informācijas sistēmas pašreizējās arhitektūras analīze un priekšlikumu sniegšana informācijas sistēmu pieejamības paaugstināšanai plānoto tehnisko apkopju un/vai tās jauninājumu uzstādīšanas laikā, ņemot vērā, informācijas sistēmas pieejamības prasības, kas noteiktas konkrētajai sistēmai.

7.3. **IT drošības audita darbu aktivitāšu sadalījums pa informācijas sistēmām un infrastruktūras komponentēm:** Tabula Nr.1 satur matricu, kurā ar "X" norādītas veicamās aktivitātes drošības un veiktspējas novērtēšanā, kā arī sistēmas rezerves kopēšanas procesa un atjaunošanas procesa novērtēšanā:

Tabula Nr.1

IS un IT infra-struktūras kompo-nentes	**IT drošības audita ietvaros veicamās novērtēšanas aktivitātes**					
	Normatīvā dokumen-tācija	ISO/IEC 27001: 2013	OSSTMM v3	OWASP v4	Rezerves kopijas un atjaunošanas process	Veikt-spējas un pieeja-mība
IIAS	X	X		X	X	X
Regulatora mājas lapa	X	X		X	X	X
STARS	X	X		X	X	X