Valstybinių miškų urėdija

VALSTYBĖS ĮMONĖ VALSTYBINIŲ MIŠKŲ URĖDIJA

Suinteresuotiems asmenims
(pranešimas CVP IS priemonėmis)

2026-11-05 Nr. 2

DĖL TIEKĖJO PATEIKTŲ KLAUSIMŲ IŠANKSTINĖJE (RINKOS) KONSULTACIJOJE (CVP IS NR. 10190220)

VĮ Valstybinių miškų urėdija (toliau – Perkančioji organizacija) vykdo **kibernetinio saugumo audito paslaugų pirkimo išankstinę (rinkos) konsultaciją** Nr. 10190220 (toliau – Rinkos konsultacija).

Perkančioji organizacija pateikia CVP IS priemonėmis gautus klausimus ir atsakymą į juos:

Eil. Nr.	Klausimas*	Atsakymas
	Paslaugų objektai ir kiekiai	
1.	**1. Vertinamų informacinių sistemų sąrašas** TS 3.2, 5.3.6 Prašome pateikti iki 40 vertinamų informacinių sistemų sąrašą arba nuasmenintą suvestinę pagal sistemų paskirtį, kritiškumą, naudotojų skaičių, technologijas, diegimo vietą ir išorinių sąsajų skaičių. Ar visoms sistemoms numatytas vienodas techninio testavimo gylis, ar daliai jų bus taikoma rizika pagrįsta atranka? Prašome nustatyti didžiausią į kainą įtrauktą sistemų skaičių ir aiškų atrankos būdą.	Dėkojame už pateiktus klausimus, pastabas ir įžvalgas dėl paskelbtos rinkos konsultacijos. Informuojame, kad Jūsų pateikti klausimai bus išnagrinėti ir apsvarstyti, įvertinant jų reikšmę planuojamo pirkimo objekto apimčiai, techninės specifikacijos reikalavimų aiškumui ir tinkamam paslaugų įsigijimui. Kviečiame, remiantis paskelbtu techninės specifikacijos projektu ir turima patirtimi, pateikti konkrečius pasiūlymus bei rekomendacijas, kurios, Jūsų vertinimu, leistų tiksliau apibrėžti paslaugų apimtį, užtikrintų aiškius ir objektyviai įvertinamus techninius reikalavimus, paslaugų teikimo organizavimą ir kitus aspektus bei sudarytų sąlygas platesniam tiekėjų dalyvavimui pirkime. Dėkojame už bendradarbiavimą ir aktyvų dalyvavimą rinkos konsultacijoje.
2.	**2. Sistemos ir jų komponentai** TS 3.2, 5.3.5–5.3.13 Prašome paaiškinti, kas laikoma viena informacine sistema ir ar atskirai skaičiuojamos jos žiniatinklio aplikacijos, API, mobiliosios aplikacijos, duomenų bazės, integracijos ir testavimo aplinkos. Ar kiekvienai tokiai daliai reikės atskiro pažeidžiamumų bei įsilaužimo testo?	
3.	**3. Infrastruktūros apimties suvestinė** TS 5.3.2–5.3.5, 5.3.8–5.3.10 Prašome pateikti orientacinius kiekius: viešų IP adresų ir domenų, vidinių IP intervalų, fizinių bei virtualių tarnybinių stočių, duomenų bazių, ugniasienių, maršrutizatorių, komutatorių, VPN sprendinių, WLAN valdiklių, prieigos taškų ir interneto svetainių. Kurie objektai būtų tikrinami visi, o kuriems taikoma reprezentatyvi imtis?	
4.	**4. Darbo vietų imtis** TS 3.2, 5.3.7 Koks yra bendras darbo vietų skaičius, nuo kurio bus skaičiuojama apie 10 proc. imtis? Prašome nustatyti minimalų ir maksimalų tikrintinų darbo vietų skaičių, imties sudarymo kriterijus ir ar pakanka	

Valstybės įmonė, Pramonės pr.11A, 51327 Kaunas.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 132340880.
Būstinės duomenys: Savanorių pr. 176, 03154 Vilnius.
Tel. (8 5) 273 4021, el. p. info@vivmu.lt

	vieno tipinio įrenginio kiekvienai vienodai valdomų darbo vietų grupei.	
5.	**5. Microsoft 365 ir intranetas** TS 5.3.11–5.3.13 Prašome nurodyti Microsoft 365 tenantų, naudotojų, administratorių, SharePoint svetainių ar svetainių rinkinių, Teams komandų ir intraneto sprendinių orientacinius kiekius, naudojamų licencijų lygius bei numatomą peržiūros imtį. Ar intraneto patikrinimas dubliuojasi su SharePoint ir Microsoft 365 patikrinimu, ir ar vienas patikrinimas gali būti naudojamas kelių reikalavimų rezultatams pagrįsti?	
6.	**6. Padaliniai ir trečiųjų šalių aplinkos** TS 3.2, 5.3.3–5.3.4, 5.3.6 Kiek regioninių padalinių ir fizinių vietų reikia aplankyti, kokios jų technologinės grupės ir kiek kelionių numatyti pasiūlymo kainoje? Prašome atskirti Užsakovo valdomus objektus nuo debesijos ar kitų tiekėjų valdomų objektų bei nurodyti, kas gaus jų rašytinius leidimus testuoti.	
Vertinimo metodika ir saugaus testavimo ribos		
7.	**7. Rizikos vertinimo ir audito aprėptis** TS 5.1.1–5.2.2 Ar rizikos analizė atliekama visos VMU mastu, ar tik atrinktoms sistemoms ir procesams? Prašome nurodyti vertinamų procesų, padalinių, dokumentų rinkinių ir planuojamų interviu orientacinį skaičių, taip pat kokių ankstesnių rizikos vertinimų bei auditų rezultatai bus pateikti. Prašome patvirtinti taikomų reikalavimų ir kontrolės priemonių sąrašą pagal NKSC audito metodiką.	
8.	**8. Black box ir white box apibrėžimas** TS 5.3.2–5.3.3, 5.3.6 Prašome apibrėžti, kurioms sistemoms taikomas black box, o kurioms white box tikrinimas, kokias paskyras ir vaidmenis gaus testuotojai, ar bus pateikiamas programinis kodas, architektūros schema ir konfigūracijų išrašai. Ar white box apima pilną kodo auditą, ar tik dokumentacijos, konfigūracijų ir suteiktų prieigų peržiūrą?	
9.	**9. Aktyvių testų ribojimai** TS 5.3.2, 5.3.6, 5.3.7, 5.3.9 Prašome nurodyti, ar gamybinėje aplinkoje leidžiamas tik neardantis DoS atsparumo vertinimas pagal architektūrą ir nustatymus, ar numatomi apkrovos testai. Kokie bus slaptažodžių bandymų apimties, greičio, trukmės, paskyrų blokavimo ir sustabdymo kriterijai? Ar TS 5.3.2 nurodytas ne trumpesnis kaip 2 valandų testas gali būti pakeistas iš anksto suderintu saugiu scenarijumi ir patikrinamu rezultatu?	

10.	**10. Žiniatinklio skenerių skaičius** TS 5.3.1, 5.3.10 Ar galima reikalavimą naudoti ne mažiau kaip tris automatizuotus žiniatinklio pažeidžiamumų skenerius pakeisti reikalavimu užtikrinti sutartą pažeidžiamumų klasių aprėptį, rankinę rezultatų patikrą ir klaidingų teigiamų radinių pašalinimą, leidžiant tiekėjui pasirinkti priemonių skaičių?	
11.	**11. El. pašto patikrinimo scenarijai** TS 5.3.11–5.3.12 Ar kenksmingo kodo, vykdomųjų failų, šifruotų priedų ir phishing nuorodų filtravimas turi būti tikrinamas tik suderintais nekenksmingais imitaciniais pavyzdžiais? Prašome nustatyti testinių gavėjų skaičių, leidžiamus domenus, testavimo langą ir atsakingus asmenis.	
12.	**12. Prieigos ir pradžios sąlygos** TS 4 skyrius, 5.3.2–5.3.13 Kuriuos pradinius duomenis, testavimo paskyras, konfigūracijų išrašus, tinklo schemas, trečiųjų šalių leidimus ir testavimo aplinkas pateiks Užsakovas? Per kokį terminą jie bus pateikti ir kaip keisis darbų grafikas, jei prieigos ar leidimai vėluos arba konkreti aplinka neleis numatyto testo?	
	Rezultatai, terminai ir kainodara	
13.	**13. Ataskaitų ir pradinių rezultatų apimtis** TS 5.1.2, 5.2.2, 5.3.14, 6 skyrius Prašome nurodyti, ar teikiamos trys apibendrintos ataskaitos su priedais, ar atskira ataskaita kiekvienai sistemai, padaliniui ir technologijų grupei. Kokiu formatu ir kokiu detalumu turi būti pateikiami skenavimo originalūs rezultatai, kaip bus apsaugoti slaptažodžiai, asmens duomenys ir išnaudojimo įrodymai, ir kokie yra objektyvūs rezultatų priėmimo kriterijai?	
14.	**14. Pakartotinis tikrinimas** TS 5.3.14, 6 skyrius Ar į pagrindinę kainą turi būti įtrauktas bent vienas po trūkumų ištaisymo atliekamas pakartotinis testavimas? Jei taip, prašome apibrėžti jo objektų ir radinių skaičių, atlikimo terminą, leidžiamą laikotarpį po pirminės ataskaitos ir rezultatų įforminimo būdą; jei ne, prašome numatyti atskirą įkainį.	
15.	**15. Kiekio pokyčiai, grafikas ir kaina** TS 3.2, 4 skyrius, 5.3, 6 skyrius Prašome patvirtinti galutinį į fiksuotą kainą įtrauktų objektų kiekį prieš pasiūlymų teikimą arba nustatyti bazinius kiekius ir vienetinius įkainius papildomiems objektams. Kaip bus keičiama kaina ir 5 mėnesių terminas, jei faktinis objektų skaičius ar	

	sudėtingumas viršys skelbiamą bazę, o Užsakovo dokumentų derinimas, prieigų suteikimas arba trečiųjų šalių leidimai užtruks?	
Tiekėjo ir specialistų kvalifikacija		
16.	**Sertifikatai pagal specialistų vaidmenis** 2 priedo 6.1; TS 5.2–5.3 Kokius minimalius reikalavimus numatote auditui vadovaujančiam asmeniui, rizikos vertintojui ir techninius įsilaužimo testus atliekančiam specialistui? Siūlome atskirti šiuos vaidmenis: auditą atliekantis asmuo turi atitikti Kibernetinio saugumo įstatymo ir NKSC audito metodikos sąlygas; saugumo valdymo kompetencijai, jei ji būtina, galėtų būti pateiktas GSLC arba lygiavertis įrodymas; techniniam testavimui – OSCP arba lygiavertis praktinių įgūdžių įrodymas. Ar kiekvienam vaidmeniui priimsite lygiaverčius sertifikatus bei kitus teisės aktų leidžiamus kompetencijos įrodymus ir nurodysite, kaip lygiavertiškumas bus vertinamas?	

***Suinteresuoto dalyvio paklausimų tekstas neredaguotas.**

Viešųjų pirkimų specialistė Rasita Milė

Rasita Milė, tel. Nr. +370 607 55275, el. paštas Rasita.Mile@vmu.lt