Specialiųjų pirkimo sąlygų 2 priedas
„Pasiūlymas“

PASIŪLYMAS
DĖL INFORMACINIŲ SISTEMŲ IR SU JOMIS SUSIJUSIŲ INFORMACINIŲ IR RYŠIŲ TECHNOLOGIJŲ PRIVILEGIJUOTŲ NAUDOTOJŲ VALDYMO PROGRAMINĖS ĮRANGOS ĮSKAITANT DIEGIMO BEI DOKUMENTŲ PARENGIMO IR (ARBA) PAPILDYMO PASLAUGAS PIRKIMO

Valstybinei augalininkystės tarnybai
prie Žemės ūkio ministerijos
Teikiama CVP IS priemonėmis

2025-04-14, 20250414
Vilnius

1 lentelė. Tiekėjo rekvizitai:

Tiekėjo pavadinimas ir kodas	*UAB IPRO LT, Įmonės kodas 303021910*
Tiekėjo adresas	*Laisvės pr. 60-1107, LT-05120 Vilnius*
PVM mokėtojo kodas	*LT100007604214*
Bankas ir sąskaitos numeris	*LT687044060007885653, AB SEB bankas, 70440*
Telefono Nr., internetinis puslapis, el. paštas	[redacted]
Asmens, pateikusio pasiūlymą CVP IS priemonėmis, vardas, pavardė, pareigos[1]	[redacted]
Ryšiams su Vykdytoju palaikyti skiriamo asmens vardas, pavardė, pareigos ir kontaktiniai telefonai	[redacted]

2 lentelė. Su pasiūlymu pateikiami dokumentai:

Eil. Nr.	Pateikto dokumento pavadinimas	Ar dokumente yra konfidenciali* informacija	Jeigu taip, kokiu pagrindu atitinkamas dokumentas ar jame nurodyta informacija yra konfidenciali?	Lapų skaičius
1.	Ši pasiūlymo forma	Taip	Asmens duomenys (telefono numeris, el. paštas)	14
2.	Nacionalinio saugumo reikalavimų atitikties deklaracija (specialiųjų pirkimo sąlygų 3 priedas)	Ne		1
3.	Programinės įrangos gamintojo išduotas patvirtinantis dokumentas (iPro LT UAB One Identity Manufacturer’s Authorization Letter .pdf)	Ne		1

[1] Jeigu pasiūlymą pasirašo ne tiekėjo vadovas, pasiūlyme pateikiama įgaliojimo skaitmeninė kopija.

* Informacija, nurodyta VPĮ 20 straipsnio 2 dalies 1, 2, 3, 4 punktuose negali būti nurodoma ir nebus laikoma konfidencialia. Tiekėjas gali nurodyti, kuri informacijos dalis pasiūlyme yra konfidenciali. Tiekėjo su pasiūlymu teikiamų dokumentų informacijos konfidencialumas gali būti nustatomas tik pagrįstais atvejais. Jeigu kils abejonių dėl tiekėjo pasiūlyme nurodytos informacijos konfidencialumo, Vykdytojas prašys tiekėją per nurodytą terminą, kuris negali būti trumpesnis kaip 3 darbo dienos, pagrįsti jos konfidencialumą. Jei tokia informacija pasiūlyme nebus nurodyta, Vykdytojas laikys, kad bet kuri pasiūlyme pateikta informacija nėra konfidenciali, išskyrus informaciją, kurią atskleidus būtų pažeisti Asmens duomenų teisinės apsaugos įstatymo reikalavimai ar Tiekėjo įsipareigojimai pagal su trečiaisiais asmenimis sudarytas sutartis.

3 lentelė. Informacija apie subtiekėjus (jeigu žinoma):

Eil. Nr.	Subtiekėjo (-ų)[2], kurio (-ių) pajėgumais tiekėjas nesiremia, pavadinimas (-ai), kontaktiniai duomenys ir jų atstovai	Nurodoma, kokius sutartinius įsipareigojimus vykdys	Apimtis EUR arba proc.
1.	....	....	....

4 lentelė. Informacija dėl pašalinimo pagrindo nustatyto 7.1.1.1 punkte:

Pašalinimo pagrindas	Tiekėjo atsakymas (pasirinkti vieną variantą):
Tiekėjas yra neatlikęs jam paskirtos baudžiamojo poveikio priemonės – uždraudimo juridiniam asmeniui dalyvauti viešuosiuose pirkimuose	☒ Patvirtinu, kad neturiu Viešųjų pirkimų įstatymo 46 straipsnio 2^1 dalyje nurodyto pašalinimo pagrindo. ☐ Patvirtinu, kad turiu Viešųjų pirkimų įstatymo 46 straipsnio 2^1 dalyje nurodytą pašalinimo pagrindą.

5 lentelė. Tiekėjo techninis pasiūlymas:

Eil. Nr.	Reikalavimų aprašymas		Siūloma rodiklio reikšmė (tiekėjas turi nurodyti siūlomą reikšmę ir kartu su pasiūlymu pateikti (išskyrus tuos reikalavimų punktus, kur yra reikalaujamas Tiekėjo įsipareigojimas) tai patvirtinančius programinės įrangos gamintojo dokumentus* arba nuorodas* į programinės įrangos gamintojo viešai skelbiamą informaciją, viešai prieinamus informacijos šaltinius)
1.	Bendri reikalavimai	1.1. Turi būti pateikta Privilegijuotų naudotojų prieigos valdymo sistema (toliau – PNPVS). 1.2. PNPVS turi leisti per PNPVS prisijungti prie ne mažiau kaip 10 kontroliuojamų IT (toliau – informacinių technologijų) sistemų neribotam privilegijuotų naudotojų skaičiui. Turės būti kontroliuojamos informacinės sistemos veikiančios klasikiniuose ir	Atitinka. Bus pateikta Privilegijuotų naudotojų prieigos valdymo sistema (toliau – PNPVS), kuri leis per PNPVS prisijungti prie ne mažiau kaip 10 kontroliuojamų informacinių technologijų (toliau – IT) sistemų neribotam privilegijuotų naudotojų skaičiaus. Galės būti kontroliuojamos informacinės sistemos veikiančios klasikiniuose ir niekuo neišskirtiniuose Windows Server (2019, 2022), CentOS Linux (7,8), RedHat Enterprise Linux 8, Ubuntu PNPVS lengvai plečiama, leidžianti padidinti (įsigyjant papildomas licencijas) kontroliuojamų IT sistemų, prie kurių jungiamasi per PNPVS, kiekį.

[2] **Subtiekėjo pasitelkimas nekeičia tiekėjo atsakomybės dėl numatomos sudaryti Sutarties įvykdymo, todėl bet kokiu atveju tiekėjas pilnai prisiima atsakomybę už subtiekėjų veiklą vykdant sutartį**

		niekuo neišskirtiniuose Windows Server (2019, 2022), CentOS Linux (7,8), RedHat Enterprise Linux 8, Ubuntu. 1.3. PNPVS turi būti lengvai plečiama, leidžianti padidinti (pvz.: įsigyjant papildomas licencijas) privilegijuotų naudotojų, kurių veiksmai būtų kontroliuojami su PNPVS, kiekį ir/arba kontroliuojamų IT sistemų, prie kurių jungiamasi per PNPVS, kiekį.	
2.	Architektūriniai reikalavimai	2.1. PNPVS turi veikti kompiuterių tinklo šliuzo (angl. gateway) tarp privilegijuotų naudotojų ir kontroliuojamų IT sistemų, prie kurių jie jungiasi, principu. PNPVS veikimui turi nereikėti diegti programinės įrangos į IT sistemas, jungimasis prie kurių yra kontroliuojamas. 2.2. PNPVS architektūra turi leisti vykdyti prieigos kontrolę prie	Atitinka. 2.1. PNPVS veikia kompiuterių tinklo šliuzo (angl. gateway) tarp privilegijuotų naudotojų ir kontroliuojamų IT sistemų, prie kurių jie jungiasi, principu. PNPVS veikimui nereikia diegti programinės įrangos į IT sistemas, jungimasis prie kurių yra kontroliuojamas. PNPVS architektūra leidžia vykdyti prieigos kontrolę prie kontroliuojamų IT sistemų (t. y. jungimasis prie šių IT sistemų gali vykti tik per PNPVS). https://docs.oneidentity.com/bundle/safeguard-for-privileged-passwords_release-notes_8.0/page/guides/releasenotes/about-safeguard-products.htm 2.3. PNPVS diegimas galimas į: 2.3.1. Kernel-based Virtual Machine (KVM); 2.3.2. Microsoft Hyper-V; 2.3.3. vSphere (VMware ESX); 2.3.4. Azure Marketplace; 2.3.5. Amazon Web Services (AWS). https://docs.oneidentity.com/bundle/safeguard-for-privileged-passwords_administration-guide_8.0/page/guides/shared/virtualappandvmwebkiosk.htm