

PREGLED POSTUPKA #18242

1 PODACI O NARUČIOCU

Naziv naručioca	MINISTARSTVO PRAVDE, LJUDSKIH I MANJINSKIH PRAVA
PIB	11070094
E-mail	kabinet@mpa.gov.me
Telefon	020/407-501
Internet adresa	mpa.gov.me
Fax	020/407-515
Adresa	ulica Vuka Karadžića 3
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Usluga podizanja nivoa bezbjednosti informacionog sistema Ministarstva pravde,ljudskihi manjinskih prava
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Oliver Bodven
Kontakt	020/407-522
Datum objave	15.04.2022. 14:00

Napomena	Usluga podizanja nivoa bezbjednosti informacionog sistema Ministarstva pravde, ljudskih i manjinskih prava- Implementacija softverskih rješenja i mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata, u cilju zaštite kritične infrastrukture Ministarstva
----------	--

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Usluga podizanja nivoa bezbjednosti informacionog sistema Ministarstva pravde, ljudskihi manjinskih prava- Implementacija softverskih rješenja i mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata, u cilju zaštite kritične infrastukture Ministarstva	15.04.2022 14:00	26.04.2022 13:00	26.04.2022 13:30	U toku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2022	MINISTARSTVO PRAVDE, LJUDSKIH I MANJINSKIH PRAVA Usluga podizanje nivoa bezbjednosti informacionog sistema Ministarstva pravde, ljudskih i manjinskih prava Implementacija softverskih rješenja i mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata, u cilju zaštite kritične infrastrukture Ministarstva 48732000 - Softverski paket za bezbjednost podataka 72226000 - Savjetodavne usluge u vezi sa testiranjem prihvaćenosti softverskog sistema 72228000 - Savjetodavne usluge u vezi sa integrisanjem hardvera 72263000 - Usluge implementacije softvera 72265000 - Usluge konfiguracije softvera	16.529,00 EUR	3.471,00 EUR	-	-	-	Jednostavna nabavka

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora. - minimum1(jedno) koja posjeduje CISSP (Certified Information Systems Security Professional) sertifikat Stručna i tehnička sposobnost dokazuje se: • dokazom o angažovanju radne snage (kopija radne knjižice, prijava za osiguranje ili ugovor o radu) i dostavljanjem traženog sertifikata	Stručna i tehnička sposobnost
Način plaćanja je: virmanski, po fakturama; Plaćanje će se izvršiti nakon završetka implementacije softverskog rješenja, uz potpisan Zapisnik o primopredaji od strane ovlaštenog lica Direktorata za IKT pravosuđa i bezbjednost podataka za stavku 1 Plaćanje će se izvršiti u 12 mjesečnih rata, u cilju obezbjeđivanja tehničke podrške za implementirano softversko rješenje, a koja počinje od dana potpisivanja Zapisnika o kvalitativno-kvantitativnom prijemu softverskog rješenja za stavku 2.	Način plaćanja
Rok plaćanja je: 30 dana od dana dostavljanja fakture nakon završetka implementacije softverskog rješenja, uz potpisan Zapisnik o primopredaji od strane ovlaštenog lica Direktorata za IKT pravosuđa i bezbjednost podataka za stavku 1. 30 dana od dana dostavljanja fakture za prethodni mjesec (12 mjeseci), u cilju obezbjeđivanja tehničke podrške za implementirano softversko rješenje, a koja počinje od dana potpisivanja Zapisnika o kvalitativno-kvantitativnom prijemu softverskog rješenja za stavku 2.	Rok plaćanja
Rok važenja ponude je 10 dana od dana otvaranja ponuda.	Rok važenja ponude
Mjesto izvršenja ugovora je Ministarstvo pravde, ljudskih i manjinskih prava, ulica Vuka Karadžića br. 3.	Mjesto izvršenja ugovora

<p>Sastavni dio ponude je popunjen i ovjeren Obrazac 2 (član 5 stav 4 Pravilnik za sprovođenje jednostavnih ("Službeni list Crne Gore" , broj 061/20, 065/20, 071/20, 74/20, 102/20 i 51/21) Potpisivanjem Obrasca 2 - izjava, ovlašteno lice ponuđača pod punom moralnom, materijalnom i krivičnom odgovornošću izjavljuje da ispunjava uslove za obavljanje djelatnosti u postupku jednostavne nabavke da: Uslovi sposobnosti privrednog subjekta: a) uslovi za obavljanje djelatnosti: • je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište. Dokazivanje uslova za obavljanje djelatnosti Ispunjenost uslova za obavljanje djelatnosti dokazuje se dostavljanjem: 1) dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlaštenom licu privrednog subjekta</p>	<p>Uslovi za obavljanje djelatnosti</p>
<p>Potpisivanjem Obrasca 2 - izjava, ovlašteno lice ponuđača pod punom moralnom, materijalnom i krivičnom odgovornošću izjavljuje da ne postoji sukob interesa definisan članom 41 Zakona o javnim nabavkama ("Službeni list Crne Gore" , broj 061/20, 065/20, 071/20, 74/20, 102/20 i 51/21)</p>	<p>Obavezni uslovi</p>
<p>Sastavni dio ponude je popunjen i ovjeren Obrazac 2 (član 5 stav 4 Pravilnik za sprovođenje jednostavnih ("Službeni list Crne Gore" , broj 061/20, 065/20, 071/20, 74/20, 102/20 i 51/21) Potpisivanjem Obrasca 2 - izjava, ovlašteno lice ponuđača pod punom moralnom, materijalnom i krivičnom odgovornošću izjavljuje da ispunjava obavezne uslove za učešće u postupku jednostavne nabavke da: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu; 2) je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje.</p>	<p>Obavezni uslovi</p>
<p>Rok izvršenja ugovora je: 30 dana od dana zaključivanja ugovora za stavku 1 i 12 mjeseci od dana implementacije za stavku 2.</p>	<p>Rok izvršenja ugovora</p>
<p>Drugi uslov: Ponuđač se mora obavezati da će imati na raspolaganju jedno lice koja će po zahtjevu Naručioca fizički pristupiti na lokaciji Naručioca i koje će biti odgovorno za pružanje usluga na lokaciji Naručioca.</p>	<p>Drugi uslovi</p>

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena
Reference ponuđača u poslednjih 5 godina, koje moraju sadržati minimalno implementaciju softverskih rješenja sa ciljem centralizovanog prikupljanja, bezbjedonosne analize i korelacije podataka generisanih od strane različitih uređaja i elemenata informaciono komunikacionog sistema, odnosno informatičke infrastrukture. Broj bodova za ovaj podkriterijum određuje se po formuli: $\text{Broj bodova} = (R_p / R_{\text{max}}) * 60$ gdje je: R_p – ponuđene reference R_{max} – maksimalni broj ponuđenih referenci

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **16.529,00 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		<p>U skladu sa Akcionim planom Strategije Sajber bezbjednosti 2018-2021. god. Ministarstvo pravde, ljudskih i manjinskih prava(u daljem tekstu Ministarstvo) je dužno, kao vlasnik kritične informatičke infrastrukture da realizuje mjeru 2.3 Implementacija mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata, pošto su budžetom za 2022. godinu planirana i obezbijeđena odgovarajuća sredstva. Indikator rezultata mjere je: Implementacija minimum jednog softverskog rješenja koje će povećati nivo monitoringa, zaštite, upravljanja ranjivostima ili mehanizama za forenziku i analizu. Dodatno, na osnovu Programa razvoja informaciono-komunikacionih tehnologija pravosuđa za period 2021-2023. godine Direktor za informaciono komunikacione tehnologije pravosuđa i bezbjednost podataka Ministarstva treba da kontinuirano sprovodi aktivnosti unapređenja sistema informacione bezbjednosti u cilju poboljšanja uvida u događaje u informaciono komunikacionom sistemu, omogućavanja jednostavnijeg i preciznijeg utvrđivanja prijetnji i incidenata, te brzog odgovora na uočene prijetnje i incidente.</p> <p>Predmet javne nabavke su konsultanske usluge, koje</p>	

uključuju analizu postojećeg stanja prikupljanja dnevnika događaja, pohranjivanja prikupljenih dnevnika događaja i analize prikupljenih dnevnika događaja, kao i implementacija namjenskog softverskog rješenja za centralizovano prikupljanje, bezbjedonosnu analizu i korelaciju podataka generisanih od strane različitih sistema i elemenata informaciono komunikacione infrastrukture ministarstva, koja je predmet odgovornosti Direktorata za informaciono komunikacione tehnologije pravosuđa i bezbjednost podataka.

Predmetno softversko rješenje treba da obezbijedi efikasno, pravovremeno i precizno uočavanje unutrašnjih i spoljašnjih informacionih prijetnji i incidenata, koje će kao rezultat omogućiti preduzimanje adekvatnih koraka u cilju pokretanja procesa otklanjanja pričinjene štete i prevencije pojavljivanja sličnih događaja u budućnosti.

Unapređenje sajber bezbjednosti informaciono komunikacionog sistema Ministarstva, kao informaciono komunikacionog sistema od posebnog značaja za državu, podrazumijeva nabavku i implementaciju rješenja koje je u mogućnosti da efikasno i bezbjedno prikupi, sačuva, obradi i prikaže željene rezultate, za sve postojeće elemente informaciono komunikacione infrastrukture, koja se sastoji od računarske infrastrukture, servera i storage uređaja sa pripadajućim servisima, zaštitne i mrežno-komunikacione opreme, kao i da bude u mogućnosti da iste operativne sposobnosti sprovede i na potencijalnim proširenjima informaciono komunikacionog sistema.

Licence za ponuđeno rješenje ne smiju biti upotrebno ograničavajuće u parametrima „događaja u sekundi“ ili „količine podataka dnevno“, čime se obezbjeđuje da tražena

licenca u potpunosti omogućiti neometanu i troškovno unaprijed poznatu upotrebu tokom trajanja licencnog perioda.

Također, neophodno je da rješenje bude bazirano na open source-u, odnosno da omogućiti kontinualan uvid u izvorni kod čime će Ministarstvo pravde, ljudskih i manjinskih prava biti u mogućnosti da u bilo kom trenutku provjeri kvalitet implementiranog rješenja u cjelosti.

Implementacijom pomenutog rješenja u okviru informaciono komunikacionog sistema Ministarstva će se obezbijediti sljedeća dodatna funkcionalnost:

- Automatizacija prikupljanja, pohrane i obrade podataka dobijenih iz različitih izvora, koje sačinjavaju elementi informaciono komunikacionog sistema
- Primjena metoda normalizacije, transformacije i korelacije nad prikupljenim podacima
- Pravilna identifikacija malicioznih, kao i potencijalno malicioznih prijetnji i pravovremeno uočavanje incidenata
- Integracija i razmjena podataka sa drugim elementima bezbjednosne infrastrukture informaciono komunikacionog sistema Ministarstva
- Uočavanje i izvještavanje o neželjenom i/ili zlonamjernom ponašanju u okviru informaciono komunikacionog sistema Ministarstva

Opšti tehnički zahtjevi

Ponuđeno rješenje mora posjedovati sljedeće tehničke karakteristike:

- Centralizovano upravljanje svim komponentama rješenja, putem jedinstvene upravljačke konzole
- Mogućnost prikupljanja, pohranjivanja, normalizacije, transformacije, korelacije i predstavljanja podataka

1	<p>Usluga podizanje nivoa bezbjednosti informacionog sistema Ministarstva pravde, ljudskih i manjinskih prava- Implementacija softverskih rješenja i mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata, u cilju zaštite kritične infrastukture Ministarstva</p>	<p>prikupljenih, iz minimalno sljedećih izvora podataka:</p> <ul style="list-style-type: none"> o Microsoft Active Directory o Microsoft 365 o Microsoft Azure o Microsoft Exchange o Microsoft SQL Server o Cisco IOS/CatOS bazirani uređaji o Juniper JunOS bazirani uređaji o Fortinet FortiGate o Oracle Database o Apache o Nginx o Qmail o Sendmail o Postfix • Prikupljanje podataka dobijenih putem sljedećih protokola: o Syslog o FTP o NetFlow o sFlow o SNMP Trap o ODBC kolektor o Prilagodljivih agenata za Windows operative sisteme • Mogućnost parsiranja standardizovanih Syslog i SyslogNG dnevnika događaja • Mogućnost parsiranja ostalih struktuiranih izvora događaja • Mogućnost definisanja i kreiranja više različitih korisnika sistema, kao i korisničkih grupa i privilegija, kojima se definiše i odvaja nadležnost različitih korisnika unutar sistema • Prikupljanje, indeksiranje i pohranjivanje podataka unutar sistema, do vremena definisanog u sistemu, a koje se može 	1,00 komplet
---	---	--	--------------

prilagoditi na različit vremenski period za različite grupe dnevnika događaja

- Skladištenje prikupljenih podataka na bezbjedan i pouzdan način, onemogućavajući korisnicima i administratorima sistema mogućnost pristupa direktnim putem
- Mogućnost pribavljanja i objedinjavanja informacija o identitetu korisnika iz više izvora (LDAP, Microsoft Active Directory, Microsoft i Oracle baza podataka, Microsoft 365 i slično)
- Mogućnost definisanja i kreiranja notifikacionih pravila, putem definisanja upita, pretraga, pragova kojima se generiše kreiranje obavještenja o uočenom događaju izabranoj grupi korisnika; rješenje dodatno treba da posjeduje predefinisana pravila o obavještavanju, koja se mogu po potrebi aktivirati
- Mogućnost pregleda, pretrage i filtriranja dnevnika događaja putem Query jezika, kao i posjedovanje predefinisanih upita prilagođenih različitim proizvođačkim i tehnološkim rješenjima
- Mogućnost kreiranja i čuvanja prilagođenih pretraga i prikaza, kao i mogućnost kreiranja grafičkih prikaza i pregleda rezultata pretrage
- Mogućnost pretrage i filtriranja prikupljenih podataka na osnovu izvora, vremenskog perioda, naziva servera ili radne stanice koja je obuhvaćena predmetnim podacima, korisničkog imena, grupe/uloge korisnika, naziva aplikacije, imena baze/foldera/fajla kojem je pristupano, tipu događaja, tipu protokola, kao i na osnovu bilo kojeg parametra koji se nalazi unutar dnevnika događaja
- Mogućnost da se iz izvršene pretrage putem prečice može kreirati pravilo za pokretanje notifikacije ili incidenta
- Posjedovanje opcije za prikupljanje dnevnika događaja i

definisanje prilagođenih parsera i normalizacija događaja i sa opreme i od proizvođača za koje nije inicijalno omogućena gotova konfiguracija, bez dodatnih troškova

- Mogućnost integracije sa eksternim rješenjima za pretragu i pronalaženje ranjivosti sistema; minimum mora da bude podržana integracija sa

- o Tenable Nessus Vulnerability Scanner

- Mogućnost integracije sa eksternim Threat Intelligence rješenjima i izvorima podataka, kao i korišćenje dobijenih informacija u cilju uočavanja i ubrzavanja reakcije na maliciozne i zlonamjerne aktivnosti; minimum mora da bude podržana integracija sa:

- o MISP

- o STIX/TAXII Threat Intelligence izvorima

- Mogućnost integracije sa IDS/IPS (Intrusion Detection System/Intrusion Prevention System) sistemima

Kao rezultat konsultanstskih usluga koje su predmet ove nabavke, Direktorat za informaciono komunikacione tehnologije pravosuđa i bezbjednost podataka Ministarstva očekuje:

- Izvještaj o postojećim mjerama prikupljanja, pohranjivanja i analize dnevnika događaja

- Implementaciju rješenja za prikupljanje, pohranjivanje i analizu dnevnika događaja, sa osobinama navedenim u prethodnom tekstu

- Projekat izvedenog stanja, nakon uspješne implementacije rješenja iz prethodne stavke

Ponuđač mora imati u vidu da će se predmetne usluge obavljati u okviru informaciono komunikacionog sistema koji je dio kritične infrastrukture, kojoj pripada i informaciono komunikacioni sistem Direktorata za informaciono

komunikacione tehnologije pravosuđa Ministarstva pravde, ljudskih i manjinskih prava.

Implementacija rješenja

Ponuđeno rješenje mora da posjeduje sposobnost rada u fizičkom i virtuelnom okruženju, „on-premise“. Dodatno, rješenje mora da podržava HA (high availability) arhitekturu, kojom je omogućena sinhronizacija podataka i indeksiranja i samih događaja, na način otporan na otkaz rada uređaja. Sve komponente softverskog rješenja moraju da budu isporučene u formi softvera koji će biti instaliran od strane ponuđača na opremi koju naručilac već posjeduje. Ponuđač je u obavezi da u ponudi dostavi minimalne tehničke zahtjeve koji su potrebni za rad predmetnog softverskog rješenja. Ponuđač mora da traženo rješenje isporuči, instalira, testira i pusti u rad na opremi koju obezbijedi naručilac. Ponuđač je dužan da obezbijedi dokumentaciju o izvedenom stanju, uputstvo o korišćenju i da izvrši obuku 3 službenika Direktorata za informaciono komunikacione tehnologije pravosuđa koji se nalaze u stalnom radnom odnosu kod naručioca, u trajanju od minimum 3 radna dana, što treba da bude uključeno u ponuđenu cijenu.

2	Usluga tehničke podrške	<p>Izabrani Ponuđač je dužan da obezbijedi tehničku podršku za implementirano softversko rješenje u periodu trajanju licence (12 mjeseci), a koja počinje od dana potpisivanja Zapisnika o kvalitativno-kvantitativnom prijemu. U okviru tog perioda treba da bude obezbijeđeno sljedeće:</p> <ul style="list-style-type: none"> • Dostupnost tehničke podrške izabranog ponuđača po principu 24/7/365 telefonski • Dostupnost tehničke podrške izabranog ponuđača putem elektronske komunikacije 	12,00 mjesec
---	-------------------------	---	--------------