



REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

KLASA: 406-01/19-03/10
URBROJ: 513-03-04-19-2

Zagreb, 12. ožujka 2019.

DOKUMENTACIJA ZA JEDNOSTAVNU NABAVU

PENETRACIJSKI TEST INFORMATIČKE INFRASTRUKTURE MINISTARSTVA FINANCIJA

Bagatelna nabava: 37/19

Naručitelj: REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

Zagreb, ožujak 2019.

1. NAZIV I SJEDIŠTE NARUČITELJA

MINISTARSTVO FINANCIJA
Katančićeva 5
10000 Zagreb

Telefon: 01 459 1315
Telefax: 01 459 1070
Internetska adresa: www.mfin.hr
Adresa elektroničke pošte: ponuda@mfin.hr

2. JEZIK

Naručitelj će voditi postupak nabave i pripremiti Dokumentaciju na hrvatskom jeziku. Ponude moraju biti pripremljene na hrvatskom jeziku i latiničnom pismu. Komunikacija tima Ponuditelja i Naručitelja se odvija na hrvatskom jeziku. Ukoliko zaposlenici Ponuditelja ne vladaju tečnim hrvatskim jezikom, obveza je Ponuditelja na svoj trošak osigurati stalnu prisutnost prevoditelja.

3. PREDMET NABAVE

Predmet nabave je Penetracijski test informatičke infrastrukture Ministarstva financija.

CPV 79417000-0 Usluge savjetovanja na području sigurnosti
Procijenjena vrijednost nabave: 198.000,00 kuna

Ponuditelj je dužan ponuditi predmet nabave s tehničkim značajkama opisanima u Tehničkoj specifikaciji koja se nalazi u prilogu i čini sastavni dio Dokumentacije jednostavne nabave (Prilog 7).

OBVEZE PONUDITELJA

Usluga podrazumijeva Penetracijski test informatičke infrastrukture Ministarstva financija na lokacijama Ministarstva u jedinstvenom računalno mrežnom komunikacijskom sustavu.

Lokacije Naručitelja: Katančićeva 5, Zagreb; Vukovarska 72, Zagreb; Frankopanska 1, Zagreb; Veslačka 4, Zagreb; Svilajska 35, Osijek; Fiorella La Guardie 13, Rijeka te Mažuranićevo šetalište 24b, Split.

Sve usluge Ponuditelj dužan je realizirati u roku do 60 dana od dana potpisa Ugovora. Ponuditelj je u ponudi dužan dostaviti podatke o projektnom timu koji će u projektu sudjelovati.

Usluge savjetovanja

Cilj usluga savjetovanja je unapređenje rada IS-a, povećanje njegove funkcionalnosti i efikasnosti te upoznavanje s mogućnostima korištenja novih IT tehnologija. Kroz ove usluge Ponuditelj mora osigurati metodološki ujednačen pristup za sljedeće potrebe Naručitelja:

- Tehnološko savjetovanje o korištenju i unapređivanju sustava
- Uvođenje novih funkcionalnosti u sustav
- Upravljanje promjenama sustava
- Unaprjeđenje performansi sustava

4. IZMJENA DOKUMENTACIJE ZA JEDNOSTAVNU NABAVU

Naručitelj može do krajnjeg roka za dostavu ponuda, prema osobnoj prosudbi ili temeljem Ponuditeljeva zahtjeva za objašnjenje Dokumentacije, izmijeniti Dokumentaciju u obliku dodatka o izmjeni. Dodatak o izmjeni Dokumentacije, Naručitelj će objaviti u elektroničkom obliku na internetskim stranicama Ministarstva financija.

5. CIJENA PONUDE

Cijena ponude mora biti izražena u kunama i pisana brojkama. U cijenu ponude bez PDV-a uračunavaju se svi troškovi i popusti. Cijenu ponude potrebno je prikazati na slijedeći način: cijena (bez PDV-a), iznos PDV-a te cijena ponude s PDV-om. Cijena ponude izražava se za cjelokupan predmet nabave. Ponuditelj treba ispuniti originalni Troškovnik (Prilog 2), te treba ponuditi sve zatražene stavke iz Troškovnika. Ponude kod kojih nisu popunjene sve stavke Troškovnika smatrat će se neprihvatljivima. Cijena ponude je nepromjenjiva za vrijeme trajanja ugovora i ne može se mijenjati ni po kojoj osnovi.

6. UVJETI I ZAHTJEVI KOJE PONUDITELJI MORAJU ISPUNITI

6.1. Ponuditelj je obavezan dostaviti Izjavu o nekažnjavanju iz Priloga 3. Dokumentacije.

Izjavu daje osoba po zakonu ovlaštena za zastupanje gospodarskog subjekta. Izjava mora biti potpisana od strane odgovorne osobe i ovjerena pečatom/štambiljem.

6.2. Ponuditelj je obavezan dostaviti Izjavu o nepostojanju poreznog duga (Prilog 4.) kojom dokazuje da je ispunio obvezu plaćanja dospjelih poreznih obveza i obveza za mirovinsko i zdravstveno osiguranje.

6.3. Ponuditelj je obavezan dostaviti Izjavu o registraciji za obavljanje djelatnosti (Prilog 5.) kojom dokazuje svoj upis u sudski, obrtni, strukovni ili drugi odgovarajući registar države sjedišta. Ponuditelj mora biti registriran za djelatnost u vezi s predmetom nabave.

6.4. Ponuditelj je obavezan dostaviti Izjavu o dostavi jamstva za uredno ispunjenje ugovora u kojoj izjavljuje da će u roku od 10 (deset) dana od dana potpisa ugovora s naručiteljem dostaviti garanciju banke ili zadužnicu ili bjanko zadužnicu kao jamstvo za uredno ispunjenje ugovora (Prilog 6).

Ukoliko jamstvo za uredno ispunjenje ugovora bude naplaćeno, a ugovor se ne raskine, Ponuditelj je obavezan dostaviti novo jamstvo u roku od 10 (deset) dana od dana poziva na dostavu, u protivnom će Naručitelj raskinuti ugovor.

6.5. Popis ugovora o izvršenim uslugama

Popis ugovora o izvršenim uslugama u godini u kojoj je započeo postupak jednostavne nabave i tijekom tri godine koje prethode toj godini. Za dokazivanje sposobnosti potrebno je dostaviti popis, potvrdu/potvrde ili izjavu, potpisane od strane odgovorne osobe i ovjerene pečatom/štambiljem. Potvrda obvezno mora sadržavati sljedeće elemente: predmet nabave (predmet ugovora), iznos, datum pružene usluge, te naziv druge ugovorne strane, naručitelja u smislu Zakona o javnoj nabavi ili privatnog subjekta.

Gospodarski subjekt mora dokazati da je pružao usluge koje su predmet ovog postupka javne nabave temeljem izvršenja najmanje tri ista ili slična ugovora u posljednje tri godine čija je pojedinačna vrijednost bila najmanje 100.000,00 kn (bez PDV-a). Pod sličnim ugovorom Naručitelj smatra ugovor čija vrijednost iznosi minimalno 100.000,00 kn (bez PDV-a), te da su u isti uključene usluge iz najmanje 2 od sljedeća 3 područja:

- penetracijsko testiranje infrastrukturnih informacijskih sustava kao što su npr. vatrozid, web poslužitelj, poslužitelj elektroničke pošte i sl.
- penetracijsko testiranje web aplikacija, web servisa, mobilnih aplikacija ili client-server aplikacija,
- forenzička analiza računalnih sustava mobilnih telefonskih uređaja nakon sigurnosnog incidenta.

Pod sličnim ugovorom ne smatraju se općenito usluge i savjetovanja iz područja sigurnosti, savjetovanje u području uvođenja sustava upravljanja informacijskom sigurnošću, analize sigurnosnih produkata, analize i savjetovanja o otkrivenim sigurnosnim ranjivostima i sl. Ovim dokazom gospodarski subjekt dokazuje tehničku i stručnu sposobnost za uredno izvršavanje usluga koje su predmet ovog nadmetanja.

6.6. Certifikati zaposlenika

Ponuditelj je obavezan u svojoj ponudi kao njen sastavni dio priložiti stručne certifikate tehničkih stručnjaka kojima dokazuje da raspolaze stručnim znanjima za izvršenje usluga iz predmeta nabave, i to najmanje slijedeće certifikate:

- ECC C/EH (Certified Ethical Hacker)
- (ISC)2 CISSP (Certified Information Systems Security Professional)
- GIAC GPEN (GIAC Penetration Tester)
- GIAC GCFE (GIAC Certified Forensic Examiner)
- GIAC GXPN (GIAC Exploit Researcher and advanced penetration tester)
- Offensive Security OSWP (Offensive Security Wireless Professional)
- Offensive Security OSCP (Offensive Security Certified Professional)
- Offensive Security OSCE (Offensive Security Certified Expert)

6.7. Popis tehničkih stručnjaka

Ponuditelj je obavezan u svojoj ponudi kao njen sastavni dio priložiti Popis tehničkih stručnjaka kojim dokazuje da će za cijelo vrijeme trajanja ugovora imati na raspolaganju najmanje 6 (šest) stručnjaka iz predmetnog područja. Tražena sposobnost dokazuje se Popisom tehničkih stručnjaka koje ponuditelj ima na raspolaganju a koji posjeduju naprijed navedene važeće certifikate i preslikama certifikata.

Ponuditelji mogu u Popisu tehničkih stručnjaka navesti i certifikate koji su jednakovrijedni traženima, koje moraju priložiti svojim ponudama, ali u tom slučaju Ponuditelji moraju dostaviti dokaz jednakovrijednosti certifikata (npr. Potvrda izdavatelja traženog certifikata ili neovisnog ovlaštenog stručnog tijela da je dostavljeni certifikat jednakovrijedan traženom i slično). Pojam važeći certifikat znači da certifikat nije vremenski istekao, ukoliko je izdan na ograničeni rok važenja. Svaki certifikat mora sadržavati ime i prezime osobe na koju glasi, te mora biti izdan od strane davatelja certifikata. Certifikati priloženi u ponudi moraju biti na hrvatskom jeziku, a ukoliko su na nekom drugom jeziku, u ponudi se mora priložiti i prijevod certifikata na hrvatski jezik izrađen po ovlaštenom sudskom tumaču. Naručitelju je prihvatljivo da ponuditelj u ponudi priloži dva ili više certifikata za jednu te istu osobu. Sve navedene osobe nositelji certifikata moraju poznavati hrvatski jezik u govoru i pismu.

6.8. Izjava o alatima, uređajima ili tehničkoj opremi

Ponuditelj mora dostaviti izjavu da posjeduje alate, uređaje i tehničku opremu za izvršenje usluga skeniranja ranjivosti računalnih sustava, komunikacijskih sustava i web aplikacija, te priložiti popis. Izjava mora biti potpisana i ovjerena pečatom/štambiljom.

6.9. Izjava ponuditelja da su usluge u cijelosti sukladne zahtjevima iz tehničke specifikacije

Ponuditelj mora dati izjavu da je ponuđena usluga u cijelosti sukladna naručiteljevim zahtjevima iz tehničke specifikacije. Izjava mora biti potpisana i ovjerena pečatom/štambiljom.

6.10. Ukoliko gospodarski subjekt pri dostavi dokumenata priloži lažne podatke kojima kao natjecatelj ili ponuditelj dokazuje da ne postoje razlozi isključenja, odnosno da ispunjava uvjete sposobnosti, ponuda mu neće biti odabrana.

7. SADRŽAJ PONUDE

Ponuda mora sadržavati:

1. Obrazac ponude, Prilog 1;
2. Ponudbeni troškovnik, Prilog 2;
3. Izjava o nekažnjavanju, Prilog 3;
4. Izjava o nepostojanju poreznog duga, Prilog 4;
5. Izjava o registraciji za obavljanje djelatnost, Prilog 5;
6. Izjava o dostavi jamstva za uredno ispunjenje ugovora, Prilog 6;
7. Izjavu da je ponuđena usluga u cijelosti sukladna zahtjevima iz tehničke specifikacije;
8. Popis ugovora o izvršenim uslugama;
9. Certifikati zaposlenika. Stručni certifikati tehničkih stručnjaka kojima dokazuje da raspolaže stručnim znanjima za izvršenje usluga iz predmeta nabave;
10. Popis tehničkih stručnjaka projektnog tima koji će u projektu sudjelovati
11. Izjava o posjedovanju alata, uređaja i tehničke opreme za uslugu Penetracijskog testa interne informatičke infrastrukture Ministarstva financija: skeniranja ranjivosti računalnih sustava, komunikacijskih sustava i web aplikacija, te priložiti popis.

8. PREUZIMANJE DOKUMENTACIJE

Ponuditelji Dokumentaciju za jednostavnu nabavu preuzimaju u elektroničkom obliku na internetskim stranicama Ministarstva financija.

9. OZNAČAVANJE PONUDE

Ponuditelj predaje ponudu napisanu neizbrisivom tintom u papirnatom obliku. Ponuda mora biti uvezana u cjelinu. Ponuda se zajedno s pripadajućom dokumentacijom izrađuje na hrvatskom jeziku i latiničnom pismu

10. DOSTAVA PONUDA

Ponude se dostavljaju u jednom primjerku. Elektronička dostava ponuda nije dopuštena.

Ponude se dostavljaju na adresu Naručitelja:

MINISTARSTVO FINACIJA

Katančićeva 5

10000 Zagreb

Ponuda se dostavlja u zatvorenoj omotnici s naznakom:

NE OTVARAJ

“Jednostavna nabava 37/19”

te adresom Ponuditelja.

Ako omotnica nije obilježena kako je to navedeno u ovim Uputama, Naručitelj se ne smatra odgovornim ako se omotnica zagubi ili prerano otvori.

Krajnji rok za dostavu ponuda je 29. ožujka 2019. godine do 12:00 sati.

11. OTVARANJE PONUDA

Ponude se otvaraju 29. ožujka 2019. godine s početkom u 12:00 sati na adresi Naručitelja.

Otvaranje ponuda nije javno. Ponude otvaraju najmanje dva člana stručnog povjerenstva. Nakon što se ponude otvore i pročitaju, ostaju kod Naručitelja i ne vraćaju se Ponuditelju.

12. POJAŠNJENJE PONUDE

Naručitelj može tijekom postupka pregleda, ocjene i usporedbe ponuda tražiti od Ponuditelja potrebna tumačenja radi pojašnjenja ponude ili otklanjanja sumnji u valjanost ponude.

Nikakve promjene u ponudi, promjene cijene, osim ispravka računske pogreške ili promjene koje bi neprihvatljivu ponudu činile prihvatljivom, Naručitelj neće zahtijevati, nuditi niti dopustiti od strane Ponuditelja.

Naručitelj će u zahtjevu za pojašnjenje ponude odrediti primjeren rok u kojem Ponuditelj treba dostaviti zatraženo objašnjenje.

Naručitelj će isključiti ponudu Ponuditelja koji unutar postavljenog roka nije dao zatraženo objašnjenje ili njegovo objašnjenje nije za Naručitelja prihvatljivo.

13. ODABIR

Naručitelj će između prihvatljivih ponuda odabrati ponudu s najnižom cijenom. Prihvatljiva ponuda je ponuda sposobnog Ponuditelja koja potpuno zadovoljava sve tražene uvjete i zahtjeve iz Dokumentacije za jednostavnu nabavu. Neprihvatljiva je ona ponuda čija cijena prelazi planirana sredstva Naručitelja. Nepravilna ponuda je ponuda koja ne ispunjava uvjete vezane za svojstvo predmeta nabave, te time ne ispunjava u cijelosti zahtjeve Naručitelja određene u Dokumentaciji za jednostavnu nabavu.

14. SKLAPANJE UGOVORA

U ovom će se postupku jednostavne nabave sklopiti Ugovor o nabavi usluga Penetracijskog testa interne informatičke infrastrukture Ministarstva financija s rokom isporuke 60 dana.

15. ROKOVI I MJESTO ISPORUKE

Rok isporuke je 60 (sezdeset) dana, a počinje teći odmah po sklapanju Ugovora.

Mjesto isporuke na lokacijama Naručiitelja: Katančićeva 5, Zagreb; Vukovarska 72, Zagreb; Frankopanska 1, Zagreb; Veslačka 4, Zagreb; Svilajska 35, Osijek; Fiorella La Guardie 13, Rijeka te Mažuranićevo šetalište 24b, Split.

Naručitelj nabavu usluga Penetracijskog testa interne informatičke infrastrukture Ministarstva financija smatra projektom i Ponuditelj je dužan osigurati vođenje projekta.

Ponuditelj treba dodijeliti voditelja projekta te izraditi terminski plan isporuke najkasnije sedam dana nakon sklapanja ugovora:

- početak projekta,
- faze projekta s popisom i opisom planiranih aktivnosti,
- kontrolne točke projekta i
- završetak projekta.

Ponuditelj je u ponudi dužan dostaviti podatke o projektnom timu koji će u projektu sudjelovati.

16. UVJETI, ROKOVI I NAČIN PLAĆANJA

Naručitelj se obvezuje plaćati temeljem ispostavljenih računa, sukladno terminskom planu aktivnosti i prethodno ovjerenom Zapisniku o primopredaji uplatom ugovorenog iznosa u korist računa Ponuditelja. Rok plaćanja je 30 (trideset) dana od dana zaprimanja računa.

17. ŽALBA

Ponuditelji nemaju pravo žalbe u postupcima jednostavne nabave.

REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

OBRAZAC PONUDE

Naručitelj: REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA
Katančićeva 5, 10000 Zagreb
OIB: 18683136487 i MB 03205991

Tvrtka ili naziv Ponuditelja: _____

Adresa Ponuditelja.....: _____

OIB Ponuditelja.....: _____

Adresa elektroničke pošte: _____

Račun Ponuditelja (IBAN) i naziv banke: _____

Predmet nabave: Penetracijski test informatičke infrastrukture
Ministarstva financija

Način nabave: Jednostavna nabava 37/19

Uvjeti i način plaćanja u kunama:

Cijena ponude bez PDV-a: _____
(brojkama)

Iznos PDV-a: _____
(brojkama)

UKUPNA cijena ponude s PDV-om: _____
(brojkama)

Rok valjanosti ponude: 60 dana

Rok isporuke: 60 dana od sklapanja Ugovora

(čitko ime i prezime ovlaštene osobe Ponuditelja)

M.P.

(potpis ovlaštene osobe Ponuditelja)

Mjesto i datum

REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

Naziv ponuditelja: _____

TROŠKOVNIK Jednostavna nabava 37/19					
Rb	Opis robe / usluge	Jedinica mjere	Količina	Jedinična cijena	Ukupno (količina x jed. cijena)
1.	Penetracijski test informatičke infrastrukture Ministarstva financija	Komplet	1		
Ukupno bez PDV-a:					
PDV:					
Ukupno s PDV-om:					

Cijena ponude mora biti iskazana u kunama kao nepromjenjiva. Ponuditelj mora popuniti troškovnik, ovjeriti ga pečatom i potpisom odgovorne osobe i priložiti ponudi.

(čitko ime i prezime ovlaštene osobe Ponuditelja)

M.P.

(potpis ovlaštene osobe Ponuditelja)

Mjesto i datum

IZJAVA O NEKAŽNJAVANJU

Ja, _____ iz _____, osobna iskaznica broj _____
(ime i prezime) (mjesto)

i ja, _____ iz _____, osobna iskaznica broj _____
(ime i prezime) (mjesto)

kao osoba ovlaštena po zakonu za zastupanje gospodarskog subjekta

(naziv gospodarskog subjekta)

pod materijalnom i kaznenom odgovornošću izjavljujem da ja osobno niti gore navedeni gospodarski subjekt nismo pravomoćno osuđeni za bilo koje od slijedećih kaznenih djela, odnosno za odgovarajuća kaznena djela prema propisima države sjedišta gospodarskog subjekta, odnosno države čiji sam državljanin:

a) sudjelovanje u zločinačkoj organizaciji, na temelju:

- članka 328. (zločinačko udruženje) i članka 329. (počinjenje kaznenog djela u sastavu zločinačkog udruženja) Kaznenog zakona

- članka 333. (udruženje za počinjenje kaznenog djela) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12)

b) korupcija, na temelju

- članka 252. (primanje mita u gospodarskom poslovanju), članka 253. (davanje mita u gospodarskom poslovanju), članka 254. (zlouporaba u postupku javne nabave), članka 291. (zlouporaba položaja i ovlasti), članka 292. (nezakonito pogodovanje), članka 293. (primanje mita), članka 294. (davanje mita), članka 295. (trgovanje utjecajem) i članka 296. (davanje mita za trgovanje utjecajem) Kaznenog zakona

- članka 294.a (primanje mita u gospodarskom poslovanju), članka 294.b (davanje mita u gospodarskom poslovanju), članka 337. (zlouporaba položaja i ovlasti), članka 338. (zlouporaba obavljanja dužnosti državne vlasti), članka 343. (protuzakonito posredovanje), članka 347. (primanje mita) i članka 348. (davanje mita) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12)

c) prijevarena, na temelju

- članka 236. (prijevarena), članka 247. (prijevarena u gospodarskom poslovanju), članka 256. (utaja poreza ili carine) i članka 258. (subvencijska prijevarena) Kaznenog zakona

- članka 224. (prijevarena), članka 293. (prijevarena u gospodarskom poslovanju) i članka 286. (utaja poreza i drugih davanja) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12)

d) terorizam ili kaznena djela povezana s terorističkim aktivnostima, na temelju

- članka 97. (terorizam), članka 99. (javno poticanje na terorizam), članka 100. (novačenje za terorizam), članka 101. (obuka za terorizam) i članka 102. (terorističko udruženje) Kaznenog zakona

- članka 169. (terorizam), članka 169.a (javno poticanje na terorizam) i članka 169.b (novačenje i obuka za terorizam) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12)

e) pranje novca i financiranje terorizma, na temelju

- članka 98. (financiranje terorizma) i članka 265. (pranje novca) Kaznenog zakona

- članka 279. (pranje novca) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12)

f) dječji rad ili druge oblike trgovanja ljudima, na temelju

- članka 106. (trgovanje ljudima) Kaznenog zakona

- članka 175. (trgovanje ljudima i ropstvo) iz Kaznenog zakona („Narodne novine“, broj 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 77/11 i 143/12).

ZA GOSPODARSKI SUBJEKT¹:

(ime i prezime ovlaštene osobe gosp. subjekta)

M.P.

(potpis)

(ime i prezime ovlaštene osobe gosp. subjekta)

M.P.

U _____, dana _____

(potpis)

¹ Ako gospodarski subjekt zastupa zakonski zastupnik sa najmanje još jednom osobom (drugim zakonskim zastupnikom, prokuristom i sl.) izjavu daju obje ovlaštene osobe.

IZJAVA O NEPOSTOJANJU POREZNOG DUGA

Ja, _____ iz _____
(ime i prezime) (adresa stanovanja)

broj osobne iskaznice _____ izdane od _____

kao odgovorna osoba _____
(naziv i adresa gospodarskog subjekta)

izjavljujem da _____
(naziv i adresa gospodarskog subjekta)

nema dugovanja po osnovi dospjelih poreznih obveza i obveza za mirovinsko i zdravstveno osiguranje.

U _____, dana _____

ZA GOSPODARSKI SUBJEKT

M.P. _____
(ime, prezime i potpis ovlaštene osobe)

IZJAVA O REGISTRACIJI ZA OBAVLJANJE DJELATNOSTI

Ja, _____ iz _____
(ime i prezime) (adresa stanovanja)

broj osobne iskaznice _____ izdane od _____

kao odgovorna osoba _____
(naziv i adresa gospodarskog subjekta)

izjavljujem da _____
(naziv i adresa gospodarskog subjekta)

registrirana za obavljanje djelatnosti koja je predmet nabave.

U _____, dana _____

ZA GOSPODARSKI SUBJEKT

M.P. _____
(ime, prezime i potpis ovlaštene osobe)

IZJAVA O DOSTAVI JAMSTVA ZA UREDNO ISPUNJENJE UGOVORA

Ja, _____ iz _____
(ime i prezime) (adresa stanovanja)

broj osobne iskaznice _____ izdane od _____

kao odgovorna osoba _____
(naziv i adresa gospodarskog subjekta)

ponuditelja izjavljujem da ćemo u roku od 10 (deset) dana od dana potpisa ugovora s Ministarstvom financija, kao naručiteljem, za nabavu

_____ (upisati predmet nabave)

dostaviti garanciju banke ili zadužnicu ili bjanko zadužnicu, kao jamstvo za uredno ispunjenje ugovora. Jamstvo za uredno ispunjenje ugovora mora biti na iznos od 10 % (deset posto) vrijednosti ugovora bez PDV-a.

Bankarska garancija će biti neopoziva, bezuvjetna, na „prvi poziv“ i „bez prigovora“.

Jamstvo za uredno ispunjenje ugovora predat ćemo u roku od 10 (deset) dana od dana potpisa ugovora s rokom valjanosti najmanje 30 (trideset) dana od dana protoka ugovornog razdoblja.

Jamstvo za uredno ispunjenje ugovora će se aktivirati u slučaju povrede ugovornih obveza.

U _____, dana _____

ZA GOSPODARSKI SUBJEKT

M.P. _____
(ime, prezime i potpis ovlaštene osobe)

TEHNIČKA SPECIFIKACIJA

U nastavku je detaljan popis zahtjeva predmeta nabave. Ponuditelj je dužan priložiti ponudi Izjavu da je ponuđena usluga u cijelosti sukladna zahtjevima iz tehničke specifikacije.

Ponuditelj mora testirati ranjivosti i penetracijska testiranja informatičke infrastrukture Ministarstva financija za 500 klijentskih računala, 107 poslužitelja (Windows i Linux) i 127 aktivnih mrežnih uređaja.

Aktivnosti

Tražene aktivnosti moraju minimalno uključivati slijedeće:

- Pasivna enumeracija
 - Preslušavanje dostupnog mrežnog prometa na danoj utičnici
 - Analiza prometa i dostupnih računala i servisa
- Aktivna enumeracija
 - Analiza mrežne topologije
 - Port skeniranje (otvoreni, zatvoreni i filtrirani portovi, aktivna računala koja odgovaraju na zahtjeve...)
 - Analiza sustava (operativni sustav, te dostupne informacije koje pruža i ako je moguće)
 - Analiza dostupnih servisa (ime servisa, te inačica ako je dostupno/a)
 - Testiranje sigurnosti dostupnih servisa automatskim postupkom
 - Testiranje sigurnosti dostupnih servisa ručnim postupkom
- Iskorištavanje (Exploitation)
 - Iskorištavanje nađenih ranjivosti na osnovu prethodne faze
 - Eskalacija privilegija (ukoliko postoji ranjivost koja se može iskoristiti)
 - Probijanje zaporki (ukoliko se dođe do zaporki prethodnim metodama)
- Izvješće: Sigurnosna provjera unutrašnje IT infrastrukture

Sva testiranja je potrebno izvršavati na lokaciji Naručitelja. Sve invazivne aktivnosti je potrebno provoditi isključivo u koordinaciji s ovlaštenim predstavnikom Naručitelja. Testiranja ne smiju biti izvršena samo automatskim specijaliziranim alatima za pronalaženje ranjivosti.

Isporuke

Nakon provođenja testiranja Ponuditelj mora predati Naručitelju detaljno izvješće koje sadrži minimalno slijedeće cjeline:

- sažetak o provedenom ispitivanju za rukovoditelje
- opseg i metodologija ispitivanja
- sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom
- općenite informacije o ispitanom informacijskom sustavu
- opis svih identificiranih ranjivosti prema razini sigurnosnog rizika
- tehničke preporuke za uklanjanje identificiranih propusta
- ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava

Ukoliko Naručitelj zahtjeva pojašnjenja izvješća Ponuditelj ih mora prezentirati.

Ponovljeno testiranje

Na zahtjev Naručitelja, nakon što Naručitelj otkloni uočene nedostatke Ponuditelj mora ponoviti parcijalno testiranje.

Obveze Naručitelja

Naručitelj će Ponuditelju osigurati korisničke račune za testiranje, te radna mjesta i mrežnu infrastrukturu.

Metodologija testiranja

Testiranje je potrebno provesti prema smjernicama PTES-a (engl. Penetration Testing Execution Standard) koji je prikazan na poveznici <http://www.pentest-standard.org/>, a sastoji se iz sljedećih faza:

Interakcija prije testiranja

Interakcija prije testiranja omogućuje definirati dva važna područja radi kvalitetne priprema za test: opseg (engl. scope) i uvjete testiranja (engl. rules of engagement): period testiranja, lokaciju, upravljanje osjetljivim podacima, vrijeme u kojem se obavlja testiranje (tijekom radnog vremena, po noći...), postupanje u slučaju problema na infrastrukturi ili u slučaju blokiranja prometa, dobivanje potrebnih dozvola za testiranje.

Skupljanje informacija

Prilikom obavljanja internog penetracijskog testa, skupljanje informacija ima znatno manji opseg od skupljanja informacija prilikom vanjskog penetracijskog testa. U slučaju internog testa, skupljanje informacija se najviše odnosi na prikupljanje korisničkih računa te na skupljanje ostalih informacija koje mogu pomoći prilikom analize ranjivosti i socijalnog inženjeringa.

Modeliranje prijetnji

Modeliranje prijetnji ne spada u proces penetracijskog testiranja, već se radi komplementarno penetracijskom testu u sklopu procedure za upravljanjem rizicima. Penetracijski test na temelju dobivene analize mogućih prijetnji pokušava vjerno emulirati potencijalnu prijetnju kako bi mogao evaluirati rizike vezane uz računalnu infrastrukturu.

Analiza ranjivosti

Prilikom testiranja interne infrastrukture ranjivosti se analiziraju na dva načina:

- Pasivna analiza ranjivosti sastoji se od promatranja mrežnog prometa te nalaženja ranjivosti u njemu.
- Aktivna analiza ranjivosti sastoji se od tri faze:
 - o automatsko testiranje
 - o ručno testiranje
 - o verifikacija rezultata

Automatsko testiranje provodi se pomoću softvera za mrežno testiranje. Također se prilikom internog testiranja koristi i skener za testiranje web aplikacija bez korisničkih računa za autentikaciju. Ručnim testiranjem se pokriva sve ono što nije obuhvaćeno automatskim testiranjem. Verifikacija rezultata se radi pomoću korelacije među rezultatima skenera te ručnom provjerom.

Iskorištavanje ranjivosti

Iskorištavanje ranjivosti je najosjetljivija faza testiranja te zahtijeva planiranje i pravilno postavljanje uvjeta testiranja prije samog početka. Iskorištavanje ranjivosti je ključan dio testiranja koji pokazuje koliki je uistinu rizik koji prijetnja može učiniti pronalaskom ranjivosti. U ovisnosti o veličini projekta i zadanim ciljevima, iskorištavanje može uključivati zaobilaženje antivirusne zaštite, IDS-a, kriptiranje i pakiranje exploita, te otkrivanje 0-day ranjivosti.

Post-eksploatacijske aktivnosti

Post-eksploatacijske aktivnosti strogo su definirane uvjetima testa. Kroz uvjete testa, moguće je kao cilj definirati sljedeće aktivnosti: eskalacija privilegija, širenje na računala koja su dostupna s osvojenog računala te pribavljanje osjetljivih informacija s poslužitelja koji su inicijalno označene kao cilj testiranja.