Výzva na predkladanie ponúk

pre zákazku s nízkou hodnotou podľa § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)

1. Verejný obstarávateľ:
Úrad podpredsedu vlády SR pre investície a informatizáciu
Štefánikova 15
811 05 Bratislava
IČO 50349287
Kontaktná osoba: JUDr. Alexandra Horná, Peter Helexa
tel. č.: 02/2092 8102, 02/2092 8256
e-mail: alexandra.horna@vicepremier.gov.sk, peter.helexa@vicepremier.gov.sk
adresa hlavnej stránky verejného obstarávateľa /URL/: https://www.vicepremier.gov.sk/

2. Zatriedenie obstarávacieho subjektu podľa zákona:
Verejný obstarávateľ podľa § 7 ods. 1 písm. a) zákona o verejnom obstarávaní.

3. Názov zákazky podľa verejného obstarávateľa:
Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe.

4. Druh zákazky (tovary/**služby**/stavebné práce):
Služby

5. Hlavné miesto dodania tovaru/**poskytnutia služieb**/uskutočnenia stavebných prác:
Úrad podpredsedu vlády SR pre investície a informatizáciu, Štefániková 15, 811 05, Bratislava.

6. Výsledok verejného obstarávania:
Zmluva podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka.

7. Opis zákazky:
Základným strategickým cieľom Koncepcie kybernetickej bezpečnosti schválenej v roku 2015 vládou SR je „otvorený, bezpečný a chránený národný kybernetický priestor, t.j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku“.

V súvislosti s elektronizáciou služieb verejnej správy (e-Government) dochádza k veľmi významnému zvýšeniu závislosti výkonu verejnej správy na informačno-komunikačných technológiách t.j. informačných systémoch verejnej správy. Z uvedeného dôvodu je nevyhnutné zaistiť vysokú úroveň kybernetickej bezpečnosti týchto systémov a zabezpečiť dôvernosť, dostupnosť a integritu spracúvaných informácií a údajov. Prevencia, včasná a adekvátna reakcia na kybernetické útoky je jedným zo základných pilierov pre zabezpečenie tohto strategického cieľa ako aj pre zachovanie dôvery občanov v e-Goverment služby.

Pre zaistenie prevencie, včasnej a adekvátnej reakcie na kybernetické útoky vo verejnej správe je potrebné disponovať primerane vybavenými odbornými pracoviskami (jednotky CSIRT). Tieto pracoviská musia zabezpečiť pokrytie všetkých významných aspektov kybernetickej bezpečnosti, ktoré majú vplyv na verejnú správu. Týmito aspektami sú najmä monitorovanie a

analýza interného kybernetického prostredia verejnej správy, monitorovanie a analýza okolia t.j. externého kybernetického prostredia mimo verejnej správy, výmena informácií o kybernetických hrozbách ako aj riešenie mimoriadnych situácií a vojnových aktov.

V zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorým sa implementuje smernica EP a rady EÚ 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii zabezpečujú prevenciu, včasnú a adekvátnu reakciu jednotky pre riešenie bezpečnostných incidentov CSIRT (Computer Security Incident Response Team). V zmysle uvedeného zákona je za kybernetickú bezpečnosť informačných systémov verejnej správy zodpovedný Úrad podpredsedu vlády SR pre investície a informatizáciu (ÚPVII), ktorý za uvedeným účelom zriaďuje Vládnu jednotku CSIRT. Vládnu jednotku CISRT bude vykonávať jednotka CSIRT.SK, ktorá bude delimitovaná z MF SR. Uvedená jednotka však nie je dostatočne organizačne a technicky vybavená tak, aby mohla plniť úlohy Vládnej jednotky CSIRT. Okrem iného je pre komplexné zabezpečenie kybernetickej bezpečnosti vo verejnej správe potrebné taktiež disponovať ďalšími vhodne organizačne a technicky vybavenými jednotkami CSIRT vo všetkých významných vecných oblastiach (interné a externé kybernetické prostredie, kybernetická obrana, spravodajská činnosť).

V súčasnej dobe absentuje sieť takýchto jednotiek CSIRT, ktoré by dokázali plniť svoje úlohy na požadovanej úrovni. Je preto nevyhnutné vybudovanie a zvýšenie odborných kapacít jednotiek CSIRT na viacerých úrovniach a oblastiach pôsobnosti definovanej zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti. Keďže jedným z cieľov Operačného programu integrovaná infraštruktúra v Prioritnej osi č. 7 je aj zvýšenie kybernetickej bezpečnosti v spoločnosti (Š.C. č. 7.9), Úrad považuje za potrebné preskúmať možnosť zabezpečenia financovania týchto potrebných zmien z vyššie uvedeného operačného programu prostredníctvom Štúdie uskutočniteľnosti, ktorá detailne popíše možné riešenie prostredníctvom národného projektu.

8. Spoločný slovník obstarávania: 71241000-9 Štúdia realizovateľnosti, poradenská služba, analýza.

9. Celkový rozsah predmetu zákazky:
Výsledkom verejného obstarávania bude zmluva o poskytnutí služieb, trvanie zmluvy na dobu určitú do 15.8.2018.

Predmetom zákazky je príprava Štúdie uskutočniteľnosti pre projekt Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe bude prílohou uvažovaného zámeru národného projektu, ktorý Úrad pripravuje a musí obsahovať všetky súčasti štúdie podľa metodiky pre projekty Operačného programu integrovaná infraštruktúra Prioritná os č. 7, vrátane časti Cost Benefit analýza, Rozpočet projektu, prílohu opodstatnenosti podľa metodiky Hodnota za peniaze a iné požadované prílohy. Dodávateľ je zároveň povinný pri súčinnosti verejného obstarávateľa nahrať príslušné časti štúdie do systému MetaIS. V prípade požiadaviek na opravy a úpravy štúdie zo strany riadiacich orgánov je dodávateľ povinný tieto úkony vykonať bez navýšenia ceny, uvedenej v jeho ponuke.

Prílohy a podklady pre vypracovanie Štúdie realizovateľnosti:

Zodpovednosť za získanie potrebných údajov (interných, aj od prípadných partnerov – NASES, MO SR, NBU a podobne) pre vypracovanie štúdie uskutočniteľnosti nesie verejný obstarávateľ Úrad podpredsedu vlády SR pre investície a informatizáciu. Potrebné údaje budú následne k dispozícii v MetaIS a budú poskytnuté úspešnému uchádzačovi.

Úlohou dodávateľa bude vypracovať všetky požadované detailné prílohy a podklady štúdie uskutočniteľnosti (uvedené v MetaIS), t.j. minimálne nasledujúce vstupy:

- Zoznam zvolených služieb
- Riziká
- Kritéria kvality
- Legislatíva
- Zoznam zainteresovaných
- Zoznam cieľov
- Princípy a požiadavky
- Test štátnej pomoci
- Biznis rozhrania
- Biznis procesy
- Biznis funkcie
- Biznis služby
- Biznis informácie
- Zoznam informačných systémov
- Aplikačné moduly
- Poskytované služby IS
- Aplikačné rozhrania
- Integrácie projektu
- Výstupy projektu
- Harmonogram projektu
- Kategórie technických problémov
- Dodávateľská podpora
- Podpora vlastnými zdrojmi
- Prostriedky v prenájme
- Podmienky udržateľnosti
- Kritické premenné

Vypracovanie štúdie uskutočniteľnosti obsahuje:

1. Detailný popis aktuálneho stavu kybernetickej bezpečnosti z pohľadu legislatívy, architektúry, organizácie, procesov a prevádzky;
2. Zhodnotenie možných alternatívnych riešení kybernetickej bezpečnosti (min. 2 ďalšie alternatívy);
3. Detailný popis budúceho stavu zvoleného / odporúčaného riešenia;
4. Ekonomická analýza a budúca prevádzka;
5. Manažérske zhrnutie a základné informácie.

Sumár aktivít a výstupov:

1. Vypracovanie Štúdie uskutočniteľnosti v minimálnom rozsahu 60 normostrán.
2. Vypracovanie Príloh a potrebných podkladov pre vypracovanie Štúdie uskutočniteľnosti (v štruktúre požiadaviek uvedených v META IS);
3. Poskytnutie súčinnosti pracovníkom ÚPVII pri vkladaní vstupov do META IS.

10. Predpokladaná hodnota zákazky v EUR bez DPH: **48 957,67 EUR bez DPH**.

11. Hlavné podmienky financovania a platobné dojednania:
Na základe faktúry dodávateľa. Splatnosť faktúry do 30 dní od jej doručenia.

12. Podmienky účasti:
- Osobné postavenie uchádzačov a záujemcov vrátane požiadaviek týkajúcich sa zápisu do profesijného alebo obchodného registra:
Doklad o oprávnení poskytovať službu v oblasti predmetu zákazky (napr. výpis z obchodného registra, živnostenského registra a pod.)
Odôvodnenie požiadaviek viažucich sa k podmienke účasti osobného postavenia: Podmienka účasti vyplýva zo zákona o verejnom obstarávaní - § 32 ods. 2 písm. e) - uchádzač predloží doklad o oprávnení poskytovať službu, ktorá zodpovedá predmetu zákazky.

Technická alebo odborná spôsobilosť:
Požiadavky na expertov:

Expert č.1 Expert na kybernetickú bezpečnosť:
- Prax v oblasti informačnej a kybernetickej bezpečnosti minimálne 5 rokov, preukazuje sa životopisom.
- Odborná spôsobilosť, držiteľ certifikátu CISSP alebo CISA alebo CISM alebo ich ekvivalentu.

Expert č. 2 Expert na programové/ projektové riadenie
- Minimálne 5 ročná prax, preukazuje sa životopisom .
- Skúsenosť s minimálne s 3 štúdiami na projekty OPIS alebo OPII.

Pre splnenie podmienky účasti technickej alebo odbornej spôsobilosti uchádzač predloží životopis experta so zoznamom relevantných projektov, ktorý bude obsahovať aj meno, priezvisko, funkciu, tel. číslo a emailovú adresu na kontaktnú osobu odberateľa služieb pre overenie údajov. Ak počas plnenia zmluvy dôjde k nahradeniu pôvodne navrhnutého experta inou osobou, uchádzač musí zabezpečiť takého experta, ktorý v rovnakej alebo väčšej miere spĺňa minimálny rozsah požiadaviek podľa tohto bodu výzvy. V prípade experta č. 1 uchádzač predloží kópiu certifikátu CISSP alebo CISA alebo CISM alebo ich ekvivalentu.

Odôvodnenie požiadaviek viažucich sa k podmienkam účasti: Podmienka účasti vyplýva zo zákona č. 343/2015 Z. z. o verejnom obstarávaní - § 34 ods. 1 písm. g).

Ak z predložených dokladov nemožno posúdiť ich platnosť alebo splnenie podmienky účasti, verejný obstarávateľ požiada uchádzača o vysvetlenie alebo doplnenie predložených dokladov. Ak uchádzač nesplní požiadavky podľa tohto bodu výzvy na predkladanie ponúk, ani po výzve na vysvetlenie alebo doplnenie chýbajúcich dokladov, bude z verejného obstarávania vylúčený a ako úspešný bude vyhodnotený uchádzač, ktorý sa umiestnil ako druhý v poradí.

13. Kritérium na vyhodnotenie ponúk:
Najnižšia cena celkom uvedená v EUR vrátane DPH. Súčasťou ponukovej ceny za poskytnutie služby musia byť všetky náklady, ktoré vzniknú uchádzačovi pri plnení predmetu zmluvy.

14. Lehota na predkladanie ponúk uplynie dňa (dátum a čas)**: 10.04.2018 o 13:00**

15. Miesto na predloženie ponúk:
Ponuky je potrebné predkladať výlučne elektronicky na emailovú adresu:
alexandra.horna@vicepremier.gov.sk, peter.helexa@vicepremier.gov.sk

16. Ponuka musí obsahovať:
1. Všetky doklady, ktorým uchádzač preukáže splnenie podmienok účasti (bod 12 výzvy).
2. Doplnený a podpísaný Návrh na plnenie kritéria určeného verejným obstarávateľom na hodnotenie ponúk – podľa bodu č. 17.

Verejný obstarávateľ po vyhodnotení ponúk bezodkladne zašle informáciu o vyhodnotení ponúk všetkým uchádzačom. Verejný obstarávateľ bude úspešného uchádzača kontaktovať telefonicky alebo mailom ihneď po vyhodnotení. S úspešným uchádzačom bude uzatvorená zmluva podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka.

17. Návrh na plnenie kritéria určeného verejným obstarávateľom na hodnotenie ponúk:

Návrh na plnenie kritéria			
Kritérium	Návrh	Sadzba DPH v zmysle platnej legislatívy	Návrh
Najnižšia konečná zmluvná cena v EUR vrátane DPH. Váha kritéria je 100 %.*	Spolu.....EUR bez DPH		Spolu.....EUR vrátane DPH
V	Dátum.....	Meno a priezvisko štatutára uchádzača alebo ním poverenej osoby	Podpis

18. Jazyk, v ktorom možno predložiť ponuky:
Štátny jazyk, slovenský jazyk.

19. Minimálna lehota, počas ktorej sú ponuky uchádzačov viazané:
Do termínu 30 dní odo dňa predkladania ponúk.

20. Zákazka sa týka projektu / programu financovaného z fondov EÚ:
Áno

21. Dátum zaslania výzvy na predkladanie ponúk:
29.03.2018