Zvýšení bezpečnosti NS-SIS II – Kyberbezpečnost 2016

Prováděcí smlouva č. PPR-11571-10/ČJ-2017-990656
k Rámcové smlouvě o poskytování technické podpory a rozvoje aplikace NS-SIS II

Smluvní strany:

Česká republika – Ministerstvo vnitra

Sídlo:	Nad Štolou 936/3, PSČ 170 34, Praha
IČO:	00007064
DIČ:	CZ00007064
Zastoupená:	plk. Mgr. Pavlem Osvaldem, ředitelem Ředitelství pro podporu výkonu služby Policejního prezidia České republiky
Bankovní spojení:	Česká národní banka č.ú. xxx
Korespondenční adresa:	Policejní prezidium ČR, ŘPVS - pošt. schr. 62/ŘPVS, 170 89 Praha 7

(dále jen „Objednatel“)

a

HEWLETT-PACKARD s.r.o.

Sídlo:	Za Brumlovkou 1559/5, 140 00 Praha 4, Michle
IČO:	17048851
DIČ:	CZ17048851
Zastoupená:	Ing. Lukášem Najmanem, jednatelem
Bankovní spojení:	Číslo účtu xxx ČSOB Praha
Korespondenční adresa:	Za Brumlovkou 1559/5, 140 00 Praha 4, Michle

(dále jen „Dodavatel“)

(společně dále také jen „Smluvní strany“, nebo jednotlivě „Smluvní strana“)

uzavřely tuto Prováděcí smlouvu (dále jen „Prováděcí smlouva“) k Rámcové smlouvě o poskytování technické podpory a rozvoje aplikace NS-SIS II ze dne 26. února 2016 (dále jen „Rámcová smlouva“) v souladu s ustanoveními zákona č. 89/2012 Sb., občanský zákoník, (dále jen „občanský zákoník“) a zákona č. 137/2006 Sb., o veřejných zakázkách (dále jen „ZVZ“, nebo „zákon o veřejných zakázkách“) k veřejné zakázce s názvem „Technická podpora a zajištění rozvoje aplikace NS-SIS II v letech 2016 - 2018“ č.j. PPR-18584-55/ČJ-2015-990656.

1. PŘEDMĚT SMLOUVY

1.1. Předmětem této Prováděcí smlouvy je závazek Dodavatele poskytnout Objednateli plnění v souladu se specifikací uvedenou v Příloze č. 1 této Prováděcí smlouvy a ve výzvě Objednatele k podání nabídky (dále též jen „Plnění“).

1.2. Objednatel se zavazuje řádně dodané Plnění převzít a zaplatit za něj dohodnutou cenu, a to způsobem definovaným v této Prováděcí smlouvě a v Rámcové smlouvě.

2.1. Celková cena za Plnění dle této Prováděcí smlouvy činí 3 012 231,00 Kč bez DPH, tj 3 644 799,51 Kč, při sazbě DPH ve výši 21%. Cena za jednotlivé položky Plnění je uvedena v Příloze č. 2 této Prováděcí smlouvy.

3. ÚČINNOST SMLOUVY

3.1. Prováděcí smlouva se uzavírá na dobu určitou, a to od uzavření Prováděcí smlouvy do 29. 12. 2017.

4. OSTATNÍ UJEDNÁNÍ

4.1. Veškerá ujednání této Prováděcí smlouvy navazují na Rámcovou smlouvu a podmínkami uvedenými v Rámcové smlouvě se řídí, tj. práva a povinnosti či skutečnosti neupravené v této Prováděcí smlouvě se řídí ustanoveními Rámcové smlouvy. V případě, že ujednání obsažené v této Prováděcí smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové smlouvě, má ujednání obsažené v této Prováděcí smlouvě přednost před ustanovením obsaženým v Rámcové smlouvě, ovšem pouze ohledně plnění sjednaného v této Prováděcí smlouvě.

4.2. Tato Prováděcí smlouva nabývá účinnosti okamžikem uzavření smlouvy, tj. okamžikem jejího podpisu poslední Smluvní stranou.

4.3. Tato Prováděcí smlouva je vyhotovena ve 4 (čtyřech) stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží 2 (dva) stejnopisy Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1 – „Specifikace předmětu plnění“
Příloha č. 2 – „Rozpočet ceny“

V Praze dne 14. 6. 2017

Objednatel:

plk. Mgr. Pavel Osvald v. r.

……..

plk. Mgr. Pavel Osvald
ředitel Ředitelství pro podporu výkonu služby
Policejního prezidia České republiky

V Praze dne 16. 6. 2017

Dodavatel:

Ing. Lukáš Najman v. r.

……..

Ing. Lukáš Najman
HEWLETT-PACKARD s.r.o.
jednatel společnosti

Příloha č. 1 – „Specifikace předmětu plnění“

V souladu s Přílohou č. 1 - Technická specifikace předmětu plnění „RÁMCOVÁ SMLOUVA o poskytování technické podpory a rozvoje aplikace NS-SIS II“ Rámcové smlouvy č. PPR-18584-55/ČJ-2015-990656, a kapitolou 3. - Plnění B – Zajišťování rozvoje aplikace systému NS-SIS II, je předmětem plnění dle této Prováděcí smlouvy rozvoj aplikace systému NS-SIS II spočívající v realizaci vybraných aktivit zahrnujících technická opatření a vytvoření dokumentů s podrobnými návody pracovních postupů, a to s cílem předcházet bezpečnostním incidentům a zajistit maximální odolnost systému NS-SIS II proti kybernetickým hrozbám.

Na základě specifikace požadavků uvedených v Zadávací dokumentaci jsou aktivity, které jsou předmětem plnění rozčleněny do 4 hlavních skupin (A – D). U každé skupiny aktivit jsou uvedeny výstupy plnění, které budou v rámci projektu dodány.

Při realizaci projektu bude vyžadována součinnost Objednatele, která je uvedena na konci tohoto dokumentu souhrnně pro celé plnění.

A) Vytvoření bezpečnostní dokumentace
Dokumentace, která vznikne v rámci plnění, bude mít za účel popsat:

- Plán ochrany kritické informační infrastruktury pro systém NS-SIS II, který bude obsahovat přehled pravidel a procedur pro zajištění ochrany systému, včetně zahrnutí jednotlivých komponent IS.
- Plán reakce na KBI (kybernetický bezpečnostní incident) v rámci systému NS-SIS II, který bude obsahovat návrh obecného postupu při řešení kybernetických útoků a způsobů reakce na ně, včetně doporučení vhodných reakcí a zajištění odpovídajících důkazů.
- Plán zvládání mimořádných událostí kybernetického systému v rámci systému NS-SIS II, který bude obsahovat základní kostru postupu pro ohodnocení rozsahu škod a určení dalších kroků pro obnovu systému (např. aktivace postupu, zastřešující kroky obnovy, deaktivace procesu, kontakty a vazba na související dokumenty).

Výstupy plnění A:
(označení typu výstupu: D – dokument, S – služba)

1. (D) Vypracovaný dokument *NS-SIS II Kyberbezpečnost 2016 - Plán ochrany kritické informační infrastruktury* (zkráceně *NS-SIS II - Plán ochrany KII*).
2. (D) Vypracovaný dokument *NS-SIS II Kyberbezpečnost 2016 - Plán reakce na kybernetický bezpečnostní incident* (zkráceně *NS-SIS II - Plán reakce na KBI*).
3. (D) Vypracovaný dokument *NS-SIS II Kyberbezpečnost 2016 - Plán zvládání mimořádných událostí kybernetického systému* (zkráceně *NS-SIS II - Zvládání mimořádných událostí*).

Uvedené dokumenty budou zařazeny do komplexního souboru dokumentů *NS-SIS II Technická a provozní dokumentace*.

B) Implementace jednotného ověřování identity uživatelů a řízení oprávnění
Správa uživatelů a přístupy administrátorů k systémům v současné době nejsou sladěné. Zajištění ověřování identity uživatelů bude provedeno realizací jednotného přístupu pro všechny správce a uživatele systému (OS). Pro jednotlivé typy prvků je požadováno vytvoření nebo využití jednotné databáze uživatelů (LDAP) a jednotného způsobu ověřování. Následně budou tyto podrobné informace předány do SIEM řešení k dalšímu vyhodnocování.

Řešení je třeba rozdělit na část pro HP-UX systémy (dále též "unixové systémy") a část pro síťové systémy. První část řešení představuje napojení HP-UX systémů na ověřování vůči MS Windows AD.
Využít lze LDAP serveru, který bude naplněn pouze uživateli (uživatelskými jmény), kteří mají mít přístup k unixovým systémům. Unixové systémy je nutné přenastavit tak, aby poskytovaly informace o uživateli z LDAP. Ověřování uživatelů bude nutné upravit tak, aby docházelo k ověření uživatelských údajů (username/password) vůči MS Windows AD.
Pokud analýza ukáže potřebu technického vybavení, mohou být užity prioritně stávající servery systému NS-SIS II, případně lze ve spolupráci s pracovníky OIPIT PP ČR vytvořit virtuální server (servery) v interním cloudu OIPIT.
Pro realizaci výše uvedeného je v rámci dodávky požadováno dodat i programové vybavení (LDAP server na unixové platformě).

Výstupy plnění B:
(označení typu výstupu: D – dokument, S – služba)

1. (D) Vypracovaný dokument *Návrh napojení NS-SIS II na Active Directory (*zkráceně *NS-SIS II – Napojení na AD),* popisující způsob řešení a rozsah pokrytí pro servery a komunikační prvky náležející NS-SIS II. V dokumentu bude rovněž uvedena případná další role LDAP dedikovaného v rámci NS-SIS II.
2. (S) Konfigurace serverů a komunikačních prvků NS-SIS II pro ověřování vůči AD dle odsouhlaseného dokumentu *NS-SIS II – Napojení na AD*. Bude ověřeno úspěšným provedením testů – viz bod 5.
3. (S) Instalace nástroje LDAP (konkrétně HPE Directory Server, nebo obdobný produkt) na jednom ze serverů s operačním systémem HP-UX dle odsouhlaseného dokumentu *NS-SIS II – Napojení na AD.* Bude zaprotokolováno v *Protokolu o instalaci Open LDAP*.
4. (D) Vypracovaný testovací scénář se třemi testovacími případy pro otestování provedené konfigurace unixových a síťových systémů.
5. (S) Provedení testů dle testovacího scénáře v bodě 4. Bude zaprotokolováno v *Protokolu o provedených testech*.
6. (D) Aktualizovaný dokument *Centrální správa uživatelských účtů – správa LDAP (*Zkráceně *NS-SIS II správa LDAP)* a to včetně přejmenování dokumentu s ohledem na plánované užití MS Active Directory.

C) Aktualizace stavu řešení SIEM vzhledem k NS-SIS II – systém pro monitorování, korelaci a správu bezpečnostních událostí, pro snížení rizik.
Řešení se požaduje v následujícím rozsahu a technické a logické návaznosti:

a) Bude provedena revize aktuálního stavu vyhodnocování bezpečnostních událostí souvisejících se systémem NS-SIS II a budou navrženy opravy. Zejména musí být zohledněny úpravy v systému NS-SIS II, které byly provedeny po předání bezpečnostního systému SIEM do provozu. Po schválení oprav odpovědnými pracovníky Objednatele (pracovníkem odpovědným za oblast bezpečnosti a pracovníkem odpovědným za provoz NS-SIS II) budou úpravy realizovány.
b) Navržení úpravy (korelační pravidla, definice reportů, prvků dashboardu) systému SIEM tak, aby byla snížena míra rizik potenciálních bezpečnostních incidentů způsobených vybranými hrozbami.
c) Ověření funkčnosti úprav nastavení, a to v rozsahu a s ohledem na provozní podmínky ICT PČR a systému SIEM.
d) Bude provedena aktualizace dokumentace systému SIEM tak, aby byly zohledněny veškeré úpravy provedené v krocích 1. a 2.

e) V případě, že budou při revizi zjištěny skutečnosti, na základě kterých je třeba udělat úpravy systému (ať již po stránce HW, SW nebo nastavení), avšak nesouvisející se systémem NSSIS II, budou odpovědnému pracovníkovi PČR předány v souhrnném dokumentu "Doporučení pro další rozvoj SIEM").

Výstupy plnění C:
(označení typu výstupu: D – dokument, S – služba)

1. (S) Provedení revize konfigurace napojení NS-SIS II na systém SIEM na straně systému NS-SIS II, navržení konfiguračních úprav (bude podloženo realizací bodu 2).
2. (D) Vypracovaný dokument *Návrh úprav konfigurace napojení NS-SIS II na systém SIEM,* který bude popisovat případné změny v SIEM, které se ovšem týkají výlučně problematiky NS-SIS II. Dokument bude rovněž obsahovat popis případných nezbytných úprav NS-SIS II.
3. (D) Budou-li v průběhu projektu identifikovány oblasti vyžadující úpravy systému SIEM, nikoliv však čistě ve vztahu k systému NS-SIS II, vypracuje Dodavatel dokument *NS-SIS II Doporučení pro Objednatele pro SIEM* (zkráceně *NS-SIS II – Doporučení pro SIEM),* ve kterém budou tyto skutečnosti zachyceny.
4. *(D)* Pokud to charakter změn provedených v bodě 3. bude vyžadovat, bude aktualizován komplexní soubor dokumentů *NS-SIS II Technická a provozní dokumentace*, a to zejména v částech *01 Souhrn* a *03-04 SUAP*.

D) Zvýšení zabezpečení aplikační vrstvy

Na základě vyhodnocení provozu NS-SIS II je možno konstatovat, že z hlediska zatížení serverů je možné sloučit provoz komponenty nssis a SIB na jeden fyzický host, přičemž ovšem obě komponenty musí zůstat logicky i z hlediska zátěže oddělené. Navrhujeme proto realizovat přeskupení serverů aplikační vrstvy, což zajistí jednak lepší využití provozovaného technického vybavení a dále vyšší možnost reakce na mimořádné události, ať již vzniklé z provozních důvodů, nebo jako důsledek bezpečnostního incidentu.

Jedním z možných řešení je umístění aplikačních serverů produkčního systému a záložní čtecí kopie na fyzických serverech (pomocí HP-UX vPars, nebo Integrity VM v6), a to vždy odděleně virtuální server pro SIB (resp. SIB4Q) a server pro nssis. Při výpadku fyzického serveru tak bude systém možno i nadále provozovat. Uvolní se tak dva fyzické servery v primární lokalitě a dva v záložní lokalitě. Uvolněné servery by bylo možno v budoucnu využít např. pro posílení dotazovací farmy, případně jako další testovací prostředí.

Možné rozdělení serverů dle této varianty (bude upřesněno technickým projektem):

DC	Fyzický server	Virtuální servery
prim.	sii10	siisb10, siins10
	sii11	siisb11, siins11
zál.	sii20	siisb20, siins20
zál. čtecí	rc-sii20	rc-siisb20, rc-siins20

V primární lokalitě bude užit jako fyzický host sii10 stávající server siisb10 a jako host sii11 stávající siisb11; servery budou připojeny do VLAN SIS2-MGMT, na nich vytvořené virtuální servery budou připojeny do stejných sítí se stejnými IP jako doposud. V záložní lokalitě bude jako host sii20 užit server siisb20; host bude připojen do VLAN SIS2-BMGMT.

Pro realizaci této aktivity nepředpokládáme nákup HW ani dalších SW licencí.

Realizace této úpravy musí zahrnovat:

a) V souladu s návrhem bude jako první krok provedeno pilotní nasazení na serveru siisb11. Pro zpracování dotazů v produkčním prostředí v části SIB bude nasazen samostatný dotazovací modul (SIB4Q) v současné době užívaný ve čtecích kopiích (a proto funkčně ověřen). Modul bude nasazen do virtuálního serveru vytvořeného na uvedeném aplikačním serveru NS-SIS II. Část nssis bude rekonfigurována tak, aby min. jeden aplikační server užíval uvedený modul pro dotazování. Výsledkem pilotního provozu v produkčním prostředí budou podrobné zátěžové charakteristiky (včetně dob odezev na dotazy) a ověření vlastností mechanismu v dlouhodobém provozu. Výsledky budou následně promítnuty do nastavení, případně dalších úprav architektury zvýšení zabezpečení aplikační vrstvy.
b) Technický návrh řešení popsaný v samostatném dokumentu (součástí bude i ověření realizace).
c) Návrh postupu realizace řešení s ohledem na minimalizaci výpadků provozu včetně ověření realizace, příprava prostředí a součinnost s odpovědnými pracovníky PČR při realizaci.
d) Aktualizace dokumentace systému NS-SIS II zohledňující provedené úpravy.
e) Popis procesů start, stop a přesunu komponent aplikační vrstvy pro správce systému, včetně popisu vytvoření serverů aplikační vrstvy pro testovací účely.

Výstupy plnění D:
(označení typu výstupu: D – dokument, S – služba, P - produkt)

1. (D) Vypracovaný dokument s názvem *NS-SIS II Kyberbezpečnost 2016 - Technický projekt zvýšení zabezpečení aplikační vrstvy (zkráceně NS-SIS II - Technický projekt AV),* obsahující návrh řešení včetně doporučeného harmonogramu.
2. (S) Příprava prostředí a součinnost s odpovědnými pracovníky PČR při realizaci změn dle odsouhlaseného dokumentu *NS-SIS II Kyberbezpečnost 2016 – Technický projekt AV*. V případě, že vlastní realizace všech doporučených kroků v uvedeném dokumentu nebude z provozních, nebo jiných důvodů na straně PČR možná do doby plánovaného ukončení projektu (tj. nejpozději do 29. 12. 2017) poskytne Dodavatel následnou součinnost v rozsahu max 10 MDs včetně aktualizace dokumentace (viz bod 5.) a to v období až do 3 měsíců od akceptace projektu.
3. (D) Aktualizovaný komplexní soubor dokumentů *NS-SIS II Technická a provozní dokumentace*, doplněný o změny provedené v systému NS-SIS II v rámci projektu a o postupy požadované v bodě e) výše.

Požadovaná součinnost Objednatele

- Jmenování odpovědných osob do rolí v rámci projektu na straně Objednatele,
- zajištění dostupnosti odpovědných osob s rozhodující pravomocí pro schválení dokumentů a kroků realizovaných v rámci dodávky,
- poskytnutí Dodavateli interních předpisů a rozhodnutí z oblasti bezpečnosti, relevantních k plnění projektu,
- aktivní účast osob odpovědných za realizaci projektu na jednáních Programového výboru NS-SIS II a osob odpovědných za oblast kybernetiské a ICT bezpečnosti na případných dalších jednáních, která budou k tomuto projektu organizována,
- včasné poskytnutí informací nutných pro úspěšnou analýzu a vypracování požadovaných dokumentů a realizaci změn,
- zajištění přístupu pracovníků Dodavatele do prostor Objednatele za účelem instalace a konfigurace dodávaných a dotčených komponent,

- realizace nezbytných nastavení v systému MS Windows Active Directory, dle schváleného dokumentu *NS-SIS II – Napojení na AD,*
- implementace změn (ve spolupráci s Dodavatelem) dle odsouhlaseného dokumentu *NS-SIS II – Technický projekt AV*,
- konfigurace komunikační infrastruktury,
- schválení testovacích scénářů a testovacích případů,
- účast odpovědného pracovníka Objednatele při provedení testů.

PŘÍLOHA Č. 2 – „ROZPOČET CENY“

Celková cena za celý předmět plnění projektu „Zvýšení bezpečnosti NS-SIS II – Kyberbezpečnost 2016“ činí **3 012 231,00 Kč bez DPH**, tj **3 644 799,51 Kč, při sazbě DPH ve výši 21%**.
V tabulce níže jsou uvedeny ceny za jednotlivé položky Plnění.

	Cena bez DPH v Kč	Sazba DPH	Cena s DPH v Kč
A) Vytvoření bezpečnostní dokumentace	748 250,00	21%	905 382,50
B) Implementace jednotného ověřování identity uživatelů a řízení oprávnění	698 400,00	21%	845 064,00
C) Aktualizace stavu řešení SIEM vzhledem k NS-SIS II – systém pro monitorování, korelaci a správu bezpečnostních událostí, pro snížení rizik.	616 000,00	21%	745 360,00
D) Zvýšení zabezpečení aplikační vrstvy	949 581,00	21%	1 148 993,01
Celkem	**3 012 231,00**	**21%**	**3 644 799,51**

Tabulka 1 Cena za jednotlivé položky Plnění

Fakturace bude provedena po dodávce a akceptaci celého předmětu plnění. Přílohou faktury bude originál akceptačního protokolu k celému předmětu plnění, podepsaný pověřenými zástupci obou Smluvních stran v souladu s Rámcovou smlouvou.