Příloha č. 1 – Specifikace předmětu plnění

Počet stran: 4

Předmětem projektu je:

a) Analýza vybraných oblastí řešení aplikace VIS/VISMail z pohledu reálného fungování bezpečnostních mechanismů - zajištění souladu se ZKB – identifikace oblastí, souladu či nesouladu se ZKB (viz uvedená tabulka), navržení řešení včetně odhadu pracnosti;

Detailní analýza technických opatření	Poznámka	Zodpovědnost
Fyzická bezpečnost	Plně v kompetenci MV	PCR
Nástroj na ochranu integrity komunikačních sítí	Komunikační sítě spadají do kompetence a zodpovědnosti PČR. IBM pouze poskytne součinnost při definování pravidel firewallů v datových centrech, kde jsou umístěna aktiva systému VIS. Nebudou řešeny LAN/WAN MV	PCR
Nástroj na ověřování identity uživatelů	IBM prověří, zda jsou politiky identifikace uživatelů a administrátorů, včetně napojení na Active Directory, v souladu s požadavky ZKB. Pro ověření nastavení politik Active Directory bude nezbytná součinnost PČR.	IBM/PCR
Nástroj na řízení přístupových oprávnění	IBM prověří nástroje pro řízení přístupových oprávnění z hlediska řízení přístupu k jednotlivým aplikacím a datům a pro čtení i zápis dat a pro změnu oprávnění a zaznamenávání použití přístupových oprávnění.	IBM/PCR
Nástroj pro ochranu před škodlivým kódem	a) komunikace mezi vnitřní a vnější sítí: je v kompetenci a zodpovědnosti PČR; b) serverů a sdílených datových úložišť: v systému VIS není nasazena na serverech a datových úložištích antivirová ochrana. IBM v rámci detailní analýzy prověří potřebu a navrhne optimální řešení antivirové ochrany; c) pracovních stanic: je v kompetenci a zodpovědnosti PČR.	IBM/PCR
Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	IBM prověří, zda auditní záznamy a způsob jejich ukládání odpovídá požadavků ZKB a v rámci detailní analýzy navrhne způsob jejich doplnění pro splnění požadavků ZKB.	IBM
Nástroj pro detekci kybernetických bezpečnostních událostí	Dodavatelem bude hodnocena možnost napojení na centrální systém detekce kybernetických bezpečnostních událostí MV Za předpokladu, že pro naplnění tohoto požadavku PČR využívá SIEM, který pro PČR v současnosti implementuje 3. strana a do kterého jsou již nyní z VIS předávané informace, Dodavatel ověří v rámci detailní analýzy způsob předávání logů z VIS a zda předávaná data jsou z pohledu ZKB dostatečná, případně navrhne nezbytné úpravy.	IBM
Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	Plně v kompetenci MV	PCR
Aplikační bezpečnost	Dodavatelem bude hodnoceno, zda aplikační bezpečnost VIS/VISMail odpovídá požadavkům ZKB. V rámci detailní analýzy bude nezbytné spolu s PČR vyjasnit, zda se v případě VIS jedná o aplikaci/systém „, které jsou přístupné z vnější sítě". V případě, že ano, provede IBM detailní analýzu a navrhne způsob: - Provádění bezpečnostních testů - Ochrany aplikací - Ochrany transakcí.	IBM

Kryptografické prostředky	Dodavatelem bude hodnoceno, zda současná kryptografická ochrana v serverech VIS/VISMail odpovídá požadavkům ZKB. IBM v rámci detailní analýzy prověří, zda používané kryptografické prostředky odpovídají požadavkům ZKB a případně navrhne potřebné úpravy. Nebude řešena případná kryptografická ochrana koncových stanic, implementovaná pro jiné účely.	IBM
Nástroj pro zajišťování úrovně dostupnosti	Pro systém VIS/VISMail IBM v rámci detailní analýzy prověří,zda používané nástroje vysoké dostunosti odpovídají požadavkům ZKB v oblastech: • vysoké dostupnosti; • odolnosti proti kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost; • zálohování, redundance řešení a zajištění náhradních technických aktiv.	IBM
Bezpečnost průmyslových a řídicích systémů	Není relevantní k VIS/VISMail Vzhledem k tomu, že v systému VIS nejsou používány průmyslové a řídicí systémy, požadavky tohoto bodu se systému VIS netýkají.	
Projektové činnosti	Koordinace,dokumentace, PM	IBM

b) V návaznosti na vypracování dokumentace MV zajištění potřebné systémové bezpečnostní dokumentace (viz uvedená tabulka) a to zejména revizí stávající bezpečnostní dokumentace VIS a její uvedení do souladu se ZKB, bezpečnostní politikou OIPIT, bezpečnostní politikou ISMS MV, normami řady ISO/IEC 27xxx ve spolupráci s Objednatelem a v případě potřeby doplněním o chybějící systémovou bezpečnostní dokumentaci.

Systémová bezpečnostní politika - návrh rozdělení oblastí	Poznámka	Zpdpovědnost
Politika systému řízení bezpečnosti informací (ISMS)		PCR
Politika organizační bezpečnosti		PCR
Politika řízení dodavatelů		PCR
Politika klasifikace aktiv	PČR: klasifikace aktiv; IBM: popíše aktiva ve VIS/VISMail v návaznosti na Metodiku	IBM/PCR
Politika bezpečnosti lidských zdrojů		PCR
Politika řízení provozu a komunikací	PČR: globální politika; IBM: řízení provozu VIS/VISMail	IBM/PCR
Politika řízení přístupu		IBM
Politika bezpečného chování uživatelů	IBM popíše v příručce VIS/VISMail	IBM/PCR
Politika zálohování a obnovy	Vložit požadavek, aby měl zálohován/obnovu vyřešen také ZC CIS	PCR/IBM
Politika bezpečného předávání a výměny informací	IBM: předávání informací VIS/VISMail	IBM
Politika řízení technických zranitelností		IBM
Politika bezpečného používání mobilních zařízení		PCR
Politika poskytování a nabývání licencí programového vybavení a informací		PCR/IBM
Politika dlouhodobého ukládání a archivace informací	IBM: dlouhodobé ukládání informací VIS/VISMail na základě politiky PČR. Existuje koncept na technologické úrovni.	PCR/IBM

Politika ochrany osobních údajů	PČR: globální politika; IBM: ochrana OÚ ve VIS/VISMail	PCR/IBM
Politika fyzické bezpečnosti		PCR
Politika bezpečnosti komunikační sítě	PČR: politika bezpečnosti datových sítí; IBM: definuje pravidla FW	PCR/IBM
Politika ochrany před škodlivým kódem	PČR: sítě a stanice; IBM: servery VIS/VISMail	PCR/IBM
Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí		PCR
Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí	PČR: politika využití a údržby SIEM; IBM: na základě analýzy popíše auditní systém VIS/VISMail	PCR/IBM
Politika bezpečného používání kryptografické ochrany	PČR: globální politika; IBM: na základě analýzy kryptografická ochrana ve VIS/VISMail	PCR/IBM
Zpráva z auditu kybernetické bezpečnosti		PCR
Zpráva z přezkoumání sytému řízení bezpečnosti informací		PCR
Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik	MV má vypracováno	PCR
Zpráva o hodnocení aktiv a rizik	MV má vypracováno	PCR
Prohlášení o aplikovatelnosti		PCR/IBM
Plán zvládání rizik		IBM
Plán rozvoje bezpečnostního povědomí	Souvisí s Bezpečnostními směrnicemi (viz tabulka Bezpečnostní směrnice)	PCR
Zvládání kybernetických bezpečnostních incidentů	IBM ověří, jestli je zvládání incidentů předepsané podle MV, odpovídající pro VIS/VISMail. Ověřit, jakým způsobem naplnit požadavky zvládání kybernetických bezpečnostních incidentů předepsané MV, lze naplnit ve VIS/VISMail.	PCR
Strategie řízení kontinuity činností	V návaznosti na Havarijní plány. Pouze pro serverovny + obecný popis obnovy klientských stanic (automatická + fyzická instalace).	PCR/IBM
Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků		PCR
Projektové činnosti	Koordinace, komunikace, dokumentace, PM, …	IBM

c) Rozpracování, kontrola a aktualizace existujícího seznamu aktiv a rizik (zpracovaných MV pro VIS) ve spolupráci s Objednatelem pro účely vytvoření relevantní dokumentace a definování potřebných opatření (pro systém VIS tj. NS-VIS a VISMail).

d) Detailní rozpracování materiálů MV vytvořených pro VIS na konkrétní popisné a jednoznačné postupy v návaznosti na existující dokumentaci:
   - Směrnice pro bezpečnostního správce;
   - Bezpečnostní směrnice pro administrátory;
   - Bezpečnostní směrnice pro uživatele;
   - Směrnice pro klasifikaci informací a dat;
   - Směrnice pro zvládání bezpečnostních incidentů;
   - Směrnice pro použití síťových služeb

Bezpečnostní směrnice VIS/VIS/Mail	Poznámka
Směrnice pro bezpečnostního správce	V návaznosti na Politiku (viz tabulka k bodu b) pouze pro VIS, aktualizace dokumentů, které IBM dodávala.
Bezpečnostní směrnice pro administrátory	V návaznosti na Politiku (viz tabulka k bodu b) pouze pro VIS, aktualizace dokumentů, které IBM dodávala.
Bezpečnostní směrnice pro uživatele	V návaznosti na Politiku (viz tabulka k bodu b) pouze pro VIS, aktualizace dokumentů, které IBM dodávala.
Směrnice pro klasifikaci informací a dat	V návaznosti na Politiku (viz tabulka k bodu b) pouze pro VIS, aktualizace dokumentů, které IBM dodávala.
Směrnice pro zvládání bezpečnostních incidentů	V návaznosti na Politiku (viz tabulka k bodu b) pouze pro VIS, aktualizace dokumentů, které IBM dodávala.
Směrnice pro použití síťových služeb	Pouze pro VIS, lokálně v rámci datových center, aktualizace dokumentů, které IBM dodávala.

e) Detailní rozpracování strategie řízení kontinuity / havarijní plán / plán obnovy pro NS-VIS/VISMail centrum = serverovou část v lokalitách Bubenečská, Strojnická a klientských aplikací až na detailní procesy a stavy systému včetně popisu úlohy jednotlivých konkrétních rolí v procesu.

Řízení kontinuity VIS/VIS/Mail	Poznámka
Ropzpracování Strategie řízení kontinuity systému VIS/VISMail	V návaznosti na vypracované dokumenty MV/PCR, aktualizace dokumentů, které IBM dodávala
Politika havarijního plánování systému VIS/VISMail	V návaznosti na vypracované dokumenty MV/PCR, aktualizace dokumentů, které IBM dodávala
Plány obnovy prostředků IT systému VIS/VISMail v lokalitě Hlavní centrum-Bubenečská	V návaznosti na vypracované dokumenty MV/PCR, aktualizace dokumentů, které IBM dodávala
Plány obnovy prostředků IT systému VIS/VISMail v lokalitě Záložní centrum-Strojnická	V návaznosti na vypracované dokumenty MV/PCR, aktualizace dokumentů, které IBM dodávala
Plány obnovy klientské stanice systému VIS/VISMail	V návaznosti na vypracované dokumenty MV/PCR,a ktualizace dokumentů, které IBM dodávala

Příloha č. 2 – Rozpočet ceny a platební podmínky

Počet stran: 2

Úhrada celkové ceny za předmět plnění dle článku 2 této Prováděcí smlouvy bude provedena následujícím způsobem:

	Kč bez DPH	Kč s DPH
Etapa I Analýza vybraných oblastí řešení aplikace VIS/VISMail z pohledu reálného fungování bezpečnostních mechanismů - zajištění souladu se ZKB – identifikace oblastí, souladu či nesouladu se ZKB, navržení řešení včetně odhadu pracnosti	2 120 838,00 Kč	2 566 213,98 Kč
Etapa II V návaznosti na vypracování dokumentace MV zajištění potřebné systémové bezpečnostní dokumentace a to zejména revizí stávající bezpečnostní dokumentace VIS a její uvedení do souladu se ZKB, bezpečnostní politikou OIPIT, bezpečnostní politikou ISMS MV, normami řady ISO/IEC 27xxx ve spolupráci s Objednatelem a v případě potřeby doplněním o chybějící systémovou bezpečnostní dokumentaci.	865 648,00 Kč	1 047 434,08 Kč
Etapa III Rozpracování, kontrola a aktualizace seznamu aktiv a rizik vypracovaného MV pro VIS ve spolupráci s Objednatelem pro účely vytvoření relevantní dokumentace a definování potřebných opatření	173 130,00 Kč	209 487,30 Kč
Etapa IV Detailní rozpracování materiálů MV vytvořených pro VIS na konkrétní popisné a jednoznačné postupy v návaznosti na existující dokumentaci: ○ Směrnice pro bezpečnostního správce; ○ Bezpečnostní směrnice pro administrátory; ○ Bezpečnostní směrnice pro uživatele; ○ Směrnice pro klasifikaci informací a dat; ○ Směrnice pro zvládání bezpečnostních incidentů; ○ Směrnice pro použití síťových služeb	649 236,00 Kč	785 575,56 Kč
Etapa V Detailní rozpracování strategie řízení kontinuity / havarijní plán / plán obnovy pro NS-VIS/VISMail centrum = serverovou část v lokalitách Bubenečská a Strojnická a klientských aplikací až na detailní procesy a stavy systému včetně popisu úlohy jednotlivých konkrétních rolí v procesu.	302 976,00 Kč	366 600,96 Kč
Etapa VI Dodávka a instalace antivirového programu pro Domino server 8.5.3 na platformě Red Hat Enterprise Linux	34 302,00 Kč	
Licence antivirového programu	182 110,00 Kč	
Instalace	***216 412,00 Kč***	***261 858,52 Kč***
CELKEM	**4 328 240,00 Kč**	**5 237 170,40 Kč**

1. Daň z přidané hodnoty bude účtována v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. Pokud se DPH na základě nové právní úpravy během smluvního období změní, výše DPH se automaticky změní v souladu s touto právní úpravou. V takovém případě Dodavatel vyúčtuje výše uvedenou cenu bez DPH a připočítá DPH v příslušné zákonem stanovené výši. Tato změna nebude považována za změnu ceny ani za změnu této Prováděcí smlouvy.

2. Kompletnost každého dodaného milníku bude potvrzena podepsáním Předávacího nebo Akceptačního protokolu vedoucím Projektu Objednatele a Dodavatele. Úhrada ceny Plnění vč. DPH bude realizována Objednatelem na základě faktur, které budou vystaveny v souladu s podepsanými Předávacími nebo Akceptačními protokoly.

3. Datem zdanitelného plnění bude datum podpisu příslušného Akceptačního protokolu, Předávacího protokolu, či datum splnění příslušné části plnění. Dodavatel je povinen po vzniku práva fakturovat, vystavit a Objednateli předat do 5 pracovních dnů ode dne podpisu příslušného protokolu fakturu ve dvojím vyhotovení.

4. Splatnost faktur je 30 dnů od data jejich prokazatelného doručení Objednateli na adresu uvedenou ve Smlouvě. V případě doručení faktur po 15. prosinci se splatnost faktur prodlužuje na 60 dnů ode dne jejich prokazatelného doručení.

5. Daňový doklad musí obsahovat číslo Rámcové smlouvy, číslo této Prováděcí smlouvy a náležitosti řádného daňového dokladu podle příslušných právních předpisů, zejména pak zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že daňový doklad nebude mít odpovídající náležitosti nebo nebude vystaven v souladu s Rámcovou smlouvou, je Objednatel oprávněn zaslat jej ve lhůtě splatnosti zpět k doplnění Dodavateli, aniž se dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu Objednateli.

6. Adresa Objednatele pro doručení daňového dokladu je:
   Policejní prezidium ČR, P.O.BOX 6, OMTZ, 150 05 Praha 5

7. Fakturovaná částka se považuje za uhrazenou okamžikem odepsání příslušné finanční částky z bankovního účtu Objednatele uvedeného v této Prováděcí smlouvě ve prospěch bankovního účtu Dodavatele uvedeného v této Prováděcí smlouvě.

8. Společně s fakturami Dodavatel dodá originály předávacích nebo akceptačních protokolů, podepsané pověřenými zástupci obou Smluvních stran dle Rámcové smlouvy. Bez předložení uvedených dokumentů Objednatel nebude fakturu Dodavatele akceptovat.

9. Objednatel neposkytuje Dodavateli finanční zálohy na předmět plnění.

10. Jestliže Objednatel nesplní své platební závazky v souladu s termínem uvedeným v této Prováděcí smlouvě, a to ani po písemném upozornění Dodavatelem, bude Dodavatel oprávněn pozastavit dodávku plnění až do zaplacení splatné pohledávky nebo si vzít bez jakékoli odpovědnosti za případné škody zpět dodané nezaplacené Produkty, Programy, Materiály i další dodané položky a zároveň využít jiných právních prostředků.

11. V případě pozastavení plnění z důvodů prodlení s platbou ze strany Objednatele nebude toto považováno za prodlení Dodavatele s plněním podle této Prováděcí smlouvy.

Příloha č. 3 – Harmonogram plnění

Počet stran: 1

Předpokládáme, že realizace výše uvedeného předmětu plnění bude trvat cca 6 měsíců od podpisu smlouvy.

Rámcový harmonogram prací je odvozen od termínu podpisu Smlouvy a závisí na splnění předpokladů a součinnosti na straně Objednatele.

	Část plnění	Trvání	Předpokládané datum ukončení
1.	Etapa I – Analýza	3-4 měsíce	Do 4 měsíců od podpisu smlouvy (polovina ledna pokud práce budou zahájeny do poloviny října 2016)
2.	Etapa II – Systémová bezpečnostní dokumentace	2-3 měsíce	Do 5 měsíců od podpisu smlouvy (do konce ledna 2016, pokud analýza bude zahájena do poloviny října).
3.	Etapa III – Seznam aktiv a rizik	1 měsíc	Do 2 měsíců od podpisu smlouvy (do konce listopadu, pokud analýza bude zahájena do poloviny října).
4.	Etapa IV – Strategie řízení kontinuity	1 měsíc	Do 1 měsíce od ukončení etapy II - akceptace systémové bezpečnostní dokumentace
5.	Etapa V – Směrnice	2 měsíce	Do 2 měsíců od ukončení etapy II - akceptace systémové bezpečnostní dokumentace.
6.	Etapa VI – Antivirové řešení pro Domino server 8.5.3 na platformě Red Hat Enterprise Linux	1 měsíc	Do 1 měsíce od podpisu smlouvy

Základní milníky projektu jsou:

a) Milník 1: Seznam rizik (konec listopadu, pokud analýza bude zahájena do poloviny října a seznam rizik vypracovaný MV bude předán ihned po podpisu smlouvy)
b) Milník 2: Výstupy Etapy I – Analýza (leden 2017 pokud práce budou zahájeny do poloviny října 2016
c) Milník 3: Systémová bezpečnostní dokumentace (konec ledna 2017, pokud analýza bude zahájena do poloviny října a dokumenty vypracované MV budou předány v polovině října)
d) Milník 4: Havarijní plány (konec února 2017 / začátkem března, pokud systémová bezpečnostní dokumentace bude akceptována do konce ledna 2017 a podklady, vstupy od PCR budou předány do 20.1.2017)
e) Milník 5: Směrnice (do poloviny dubna, pokud systémová bezpečnostní dokumentace bude akceptována do konce ledna 2017 a materiály vypracované MV budou předány také do konce ledna 2017)

Konkrétní harmonogram plnění bude vypracován Dodavatelem v souladu s tímto Rámcovým harmonogramem do jednoho týdne od podpisu Smlouvy.

Práce mohou být realizovány ve výše uvedených termínech za předpokladu, že nedojde ke změně zadání ze strany Objednatele a že budou splněny Podmínky a předpoklady a součinnosti uvedené v této Prováděcí smlouvě a to v požadovaných termínech.

V případě nedodržení výše uvedených termínů, nebo neposkytnutí potřebné spolupráce, součinnosti ze strany Objednatele budou tyto termíny přiměřeně prodlouženy nebo posunuty.

Harmonogram může být upraven též na základě vzájemné písemné dohody.

Příloha č. 4 – Řídící struktura projektu

Počet stran: 2

	Řídící rada Projektu	
Sponzor Projektu Objednatele		**Sponzor Projektu Dodavatele**
Manažer Projektu Objednatele		**Vedoucí projektu Dodavatele**
Vedoucí Projektu Objednatele		
Projektový tým Objednatele		**Projektový tým Dodavatele**
Gestor, správce bezpečnosti Provozní tým Věcný tým Bezpečnostní tým		Konzultant bezpečnosti Specialisté systému VIS

Řídící rada	Rozhoduje o klíčových otázkách Projektu, změně harmonogramu a změně rozpočtu. Členy řídící rady jsou sponzoři Projektu, projektový manažer, vedoucí Projektu obou Smluvních stran a dva zástupci každé Smluvní strany. Řídící rada je konečnou instancí pro změnová řízení. Řídící rada kontroluje řízení Projektu.

Klíčové role projektu na straně Objednatele

Sponzor Projektu	***Vrcholový pracovník*** Sponzor projektu je pracovník vrcholového vedení Objednatele/Dodavatele, který má rozhodovací pravomoc a současně je odpovědný za úspěšné ukončení projektu. ▪ Účastní se schůzek Řídící rady projektu ▪ Odpovídá zejména za zajištění finančních zdrojů, zajištění včasného podpisu smluv resp. dodatků. ▪ Zajišťuje podporu projektu v rámci Objednatele/Dodavatele, splnění podmínek a předpokladů jeho realizace a nutné součinnosti v termínech potřebných pro projekt, ▪ Provádí strategická rozhodnutí, která mají vliv na úspěšnost projektu a informuje vedení Objednatele/Dodavatele o průběhu projektu. ▪ Závazně podepisuje požadavky na změnu, které jsou pro projekt zásadní a byly schváleny Řídícím výborem.
Manažer Projektu	***Vrcholový pracovník*** ▪ Má konečnou pravomoc pro určení priorit, urovnání otevřených problémů. V případě rozporů eskaluje řešení na vyšší úroveň řízení v rámci resortu MV a PČR. ▪ Přebírá materiály předané druhou smluvní stranou. ▪ Má konečnou pravomoc pro rozhodování o změnách v projektu, které nemají vliv na smluvní vztahy mezi Objednatelem a Dodavatelem. ▪ Prosazuje systém VIS v podmínkách resortu Ministerstva vnitra. ▪ Jmenuje a odvolává členy ŘR za Objednatele. ▪ Projektový manažer Objednatele svolává a řídí zasedání společného orgánu ŘR. ▪ Zajišťuje vrcholové řízení projektu dle schváleného rozpočtu, harmonogramu a rozsahu implementace ▪ Koordinuje činnosti na mimorezortní úrovni. ▪ Rozhoduje ve sporných případech ve vztahu k MV.

Vedoucí Projektu	***Hlavním úkolem vedoucího Projektu je koordinace práce jednotlivých týmů a přijímání rozhodnutí přesahující kompetence těchto týmů.*** ▪ Koordinuje práci jednotlivých členů projektového týmu a pravidelně informuje manažera Projektu o splněných úkolech či případných problémech. ▪ Přebírá materiály předané druhou Smluvní stranou. ▪ Je zodpovědný za akceptace dílčích předmětů plnění a jejich částí. ▪ Je odpovědný Řídící radě. ▪ Kontroluje průběžně postup všech fází a částí Projektu. ▪ Přijímá návrhy jednotlivých členů týmu a rozhoduje o nich v rámci svých kompetencí, případně je předkládá k rozhodnutí ŘR. ▪ Připravuje materiály pro jednání ŘR. ▪ Schvaluje harmonogramy dílčích fází Projektu ▪ Svolává pravidelně (minimálně 1x týdně), případně dle potřeby, schůzky vedení Projektu.
Gestor, správce bezpečnosti	Je zodpovědný za správnost předaných informací, specifikace zadání, požadavků, předání dokumentů vypracovaných MV, PCR. A dále pak za věcné připomínky k předaným výstupům, dokumentům. Poskytuje stanovisko nebo rozhodnutí zadavatele v případě nejednoznačných požadavků na bezpečnost nebo výklad v případě nejasných interních předpisů.

Objednatel zajistí pracovníky pro každou z výše uvedených klíčových rolí Projektu (jmenuje pracovníky, kteří budou Dodavateli k dispozici po celou dobu Projektu). Objednatel si může přizvat zástupce třetích dotčených stran (externích systémů), podílejících se na vízovém procesu.

Klíčové role projektu na straně Dodavatele

Vedoucí Projektu	Je zodpovědný za řízení projektu v rámci schváleného rozpočtu, harmonogramu a rozsahu. Je zodpovědný akceptace dílčích předmětů plnění a jejich částí. Je odpovědný řídící radě.
Konzultant bezpečnosti	Je zodpovědný za stanovení požadavků na systém VIS z hledisky ZkB, vypracování odpovídajících částí systémové bezpečnostní dokumentace a ostatních materiálů dle této smlouvy na základě informací získaných z předané dokumentace MV/PČR, interview s pověřenými pracovníky MV/PČR a interview s pověřenými pracovníky dodavatele, podílejícími se na projektu VIS (systémech NS-Vis a VISmail). Je zodpovědný za zapracování věcných připomínek k předané bezpečnostní dokumentaci po jejich projednání a vzájemném odsouhlasení.

Akceptační komise

Akceptační komise se skládá z:

- projektového manažera Objednatele,
- vedoucího projektu Objednatele,
- vedoucího projektu Dodavatele,
- garanta, správce bezpečnosti Objednatele,
- konzultanta bezpečnosti Dodavatele,

případně Sponzorů projektu.

Po dohodě mohou být na jednání akceptační komise přizváni další členové projektového týmu.

Příloha č. 5 – Součinnost Objednatele

Počet stran: 1

1. Objednatel poskytne aktuální bezpečnostní dokumentaci, organizační strukturu, popis bezpečnostních procesů, popis architektury implementovaných bezpečnostních systémů a další dokumenty relevantní předmětu plnění.
2. Objednatel vytvoří konkrétní bezpečnostní dokumenty v zodpovědnosti PCR viz Příloha č.1 této prováděcí smlouvy v požadovaných termínech dle harmonogramu
3. Všechny činnosti zejména interview s pracovníky Objednatele, (studium dokumentace/systému VIS na místě, další jednání) se budou konat na pracovišti Objednatele v Praze.
4. Objednatel po celou dobu projektu:

- vytvoří pro realizační tým organizační a věcné podmínky pro naplnění součinnosti Objednatele.
- Nese odpovědnost za správnost obsahu existujících dat a číselníků a jejich předání Dodavateli v požadovaných termínech.
- ponese odpovědnost a náklady za části označené v Příloze 1 v zodpovědnosti PCR.
- poskytne potřebné informace, specifikace požadavků nezbytné pro vypracování analýzy souladu systému VIS (NS-VIS a VIS MAIL) se ZKB včetně nezbytných konzultací k těmto specifikacím, požadavkům.
- nese odpovědnost za správnost a kompletnost předaných dokumentů a dalších směrnic a metodických pokynů nezbytných pro plnění předmětu smlouvy.

5. Objednatel je dále povinen:

- jmenovat členy Řídící rady, Manažera a Vedoucího projektu a gestora bezpečnosti nejpozději do jednoho týdne od podpisu Smlouvy a udělit jim patřičné pravomoci.
- zajistit přístup zástupcům Dodavatele do prostor Objednatele, kde jsou instalovaná zařízení Dodavatele, v odůvodněných případech i mimo řádnou pracovní dobu Objednatele.

Objednatel se dále zavazuje k následující součinnosti:

a) Správa účtů uživatelů VIS (NS-VIS a VIS MAIL) v Active Directory Policie ČR
b) Uvolňování pracovníků, jmenovaných osob/gestorů a zástupců uživatelů Objednatele podle potřeb Projektu, a to alespoň po dobu od jmenování do předání předmětu plnění do užívání.
c) Objednatel se bude podílet na aktualizaci a připomínkování předaných dokumentů, výstupů analýzy a jejich pracovních verzí a případném ověřování v provozu a vzhledem k příslušným interním směrnicím a dokumentům.
d) Objednatel souhlasí s posuzováním a zasláním vyjádření k předkládaným dokumentům od Dodavatele do 3 - 5 pracovních dnů podle obsahu a rozsahu pokud nebude dohodnuto jinak.
e) Zabezpečení účasti klíčových rolí na pravidelných projektových schůzkách jednou týdně a setkání s ostatními členy týmu do příštího pracovního dne a odbornými pracovníky a zástupci uživatelů systému VIS (NS-VIS a VIS MAIL) do 2 pracovních dnů po zadání požadavku na setkání, pokud nebude dohodnuto jinak.