**Príloha č. 1**

**Opis predmetu zákazky**

1 Predmet zákazky

Názov predmetu zákazky: „B**ezpečnostné testovanie SIPS ZUC**“

2 Opis predmetu zákazky

2.1 **Informácie o informačnom systéme (ďalej len IS) potrebné pre ocenenie prác:**

2.1.1 Lokalita, v ktorej bude testovanie prebiehať: ústredie NBS (ul. Imricha Karvaša 1, Bratislava).

2.1.2 Používatelia: interní zamestnanci NBS,

2.1.3 Používateľské roly: 1 (1 používateľská rola pre správcov systému)

2.1.4 Aplikačný server: 1 (technológie: Linux, Apache, Tomcat, Java 8)

2.1.5 Funkčné oblasti (v zátvorke je uvedený približný počet stránok; 90% stránok je read-only, u ostatných stránok je priemerný počet vstupov na stránke je 3-4):

* Vstupné SEPA súbory (2)
* Výstupné SEPA súbory (2)
* Vstupné T2 súbory (2)
* Výstupné T2 súbory (2)
* Správa používateľov (4)
* Autentifikácia (1)
* Parametre ZUC (2)
* Správa servera (3)
* Asynchrónne procesy (3)
* Prehľad prenášaných objektov z/na KS (3)
* Výmaz starých údajov z databázy (2)
* Zaznamenávanie vykonaných udalostí (2)
* Správa procesov (2)
* Rozosielanie oznámení (3)
* Prehľad prijatých správ (2)

2.1.6 Architektúra SIPS ZUC:

* aplikácia (platforma Java, Spring framework)
* web rozhranie pre správu
* komunikačné (klientské) API rozhranie (vstupno-výstupná komunikácia s inou časťou IS prostredníctvom REST architektúry) – predmetom testu sú len základné vlastnosti komunikačného rozhrania
* samostatný databázový server (nie je predmetom bezpečnostného testovania)

2.1.7 Niektoré použité bezpečnostné mechanizmy:

* protokol TLS, čipové karty pre používateľov, dvojfaktorová autentifikácia používateľov (klientska autentifikácia v TLS, integrácie s AD), elektronický podpis, zoznam bezpečnostne významných udalostí, ochrana údajov (záznamov alebo tabuliek) v databáze

2.2 **Cieľ bezpečnostného testovania:**

2.2.1 Cieľom testovania je zhodnotiť ochranu údajov v aplikácii (používatelia majú prístup len k údajom a funkciám, ku ktorým majú mať prístup), otestovať bezpečnosť aplikácie a bezpečnostných riešení, identifikovať zraniteľnosti, vrátane návrhu opatrení na nápravu. Testovanie má zhodnotiť či bezpečnostné mechanizmy v aplikácii umožňujú v dostatočnej miere naplniť bezpečnostné ciele kladené na danú aplikáciu.

2.2.2 Úspešný uchádzač vyhotoví požadovanú dokumentáciu v slovenskom, českom alebo anglickom jazyku v elektronickej forme vo formátoch aplikačných programov Microsoft Word, Excel, resp. vo formáte PDF.

2.3 **Požiadavky na rozsah prác – fáza A (časový rozsah max. 3 týždne, pričom fáza A musí prebehnúť v termíne od 11.11.2019 do 29.11.2019):**

2.3.1 posúdenie implementovaných bezpečnostných riešení pre naplnenie bezpečnostných cieľov v oblastiach:

* autentifikácia používateľov
* riadenie prístupu k funkciám aplikácie a údajom
* dôvernosť a autentickosť údajov / dokumentov
* správa používateľov
* správa kľúčov a certifikátov

2.3.2 vykonanie bezpečnostného testovania aplikácie, vrátane jej rozhraní a všetkých komponentov, na ktorých je aplikácia prevádzkovaná:

* testovanie zraniteľností: minimálne v rozsahu OWASP Testing Guide v4, v akom sú príslušné sekcie relevantné pre infraštruktúru a funkcie testovaného systému
* penetračné testovanie: bez pridelených oprávnení aj s pridelenými používateľskými oprávneniami
* testovanie bude vykonané z pohľadu všetkých rolí v aplikácii
* testovanie pokryje všetky funkcie aplikácie
* manuálne overenie všetkých identifikovaných zraniteľností (nielen výstup automatizovaného skenovania)
* bezpečnostný audit konfigurácie vybraných softvérových komponentov servera (Apache, Tomcat); pri realizácii obstarávateľ na požiadanie poskytne príslušné konfiguračné súbory a parametre

2.3.3 vypracovanie dokumentácie obsahujúcej (štruktúra a rozsah dokumentácie musí zodpovedať, resp. pokrývať štruktúru odporučenú v OWASP Testing Guide v4) najmä:

* zhodnotenie bezpečnosti aplikácie, vrátane zhodnotenia naplnenia bezpečnostných cieľov
* vyhodnotenie jednotlivých oblastí testovania (na úrovní sekcií OWASP Testing Guide v4) a všetkých ostatných realizovaných testov v súlade s požiadavkami a ponukou na rozsah a spôsob testovania
* popis vykonaných testov a ich výsledkov, vrátane získaných podkladov pre jednotlivé zistenia a časových údajov (kedy test prebiehal)
* zhodnotenie jednotlivých zistení (s použitím škály Critical/High/Medium/Low/Informative, zohľadňujúcej potenciálne dopady zneužitia, potrebné schopností útočníka a pod.)
* konkrétne odporúčania na nápravu

2.3.4 prezentácia výsledkov testovania v priestoroch obstarávateľa

2.4 **Požiadavky na rozsah prác – fáza B (časový rozsah max. 1 týždeň):**

2.4.1 preverenie upraveného systému z hľadiska (predtým) identifikovaných nedostatkov

2.4.2 vypracovanie záverečného zhodnotenia bezpečnosti IS, vrátane zhodnotenia naplnenia bezpečnostných cieľov

2.5 **Požiadavky na rozsah prác – voliteľne čerpané konzultačné hodiny (max. 10 hodín):**

2.5.1 poskytnutie požadovaného počtu konzultačných hodín k posúdeniu, návrhu a implementácie bezpečnostných opatrení podľa požiadaviek obstarávateľa

2.6 **Spôsob realizácie:**

2.6.1 Technické detaily testovania – testovacie prostredie, čas, rozsah a spôsob vykonania konkrétnych testov – budú dohodnuté pred alebo počas realizácie projektu.

2.6.2 Uchádzač a verejný obstarávateľ spoločne preveria pripravenosť prostredia na bezpečnostné testovanie, po vzájomnej dohode obvykle týždeň pred začatím fázy A.

2.6.3 Verejný obstarávateľ poskytne úspešnému uchádzačovi používateľskú dokumentáciu ako aj potrebnú technickú dokumentáciu aplikácie.

2.6.4 Verejný obstarávateľ poskytne pre potreby testovania 1 používateľský počítač so štandardnou konfiguráciou používanou verejným obstarávateľom. Úspešný uchádzač použije na testovanie s použitím nástrojov potrebných pre výkon bezpečnostného testovania vlastné prenosné počítače.

2.6.5 Pre získanie relevantných konfiguračných parametrov v rámci bezpečnostného auditu konfigurácie vybraných softvérových komponentov servera poskytne úspešný uchádzač verejnému obstarávateľovi skripty na automatizovaný zber týchto parametrov na začiatku fázy A.

2.6.6 Úspešný uchádzač vykoná bezpečnostné testovanie v priestoroch verejného obstarávateľa.