ЗАПИТ НА НАДАННЯ ВИСЛОВЛЕНЬ ЗАЦІКАВЛЕНОСТІ
(REoI № MF-IC-14)
(консультаційні послуги, індивідуальний консультант)

УКРАЇНА
ПРОЕКТ ЗМІЦНЕННЯ УПРАВЛІННЯ ДЕРЖАВНИМИ РЕСУРСАМИ ЧАСТИНИ В «ПІДТРИМКА ВПРОВАДЖЕННЯ СТРАТЕГІЇ УПРАВЛІННЯ ДЕРЖАВНИМИ ФІНАНСАМИ» (ПОРЯДКОВИЙ НОМЕР ПРОЕКТУ P161586)

Грант № TF0A5324

Назва завдання: Консультант з інформаційної кібербезпеки з підтримки документування

№ завдання (за Планом закупівель): MF-IC-14

Уряд України отримав фінансування з боку Міжнародного банку реконструкції та розвитку (далі – Світовий банк), який виступає адміністратором коштів гранту, наданого Європейською комісією від імені Європейського Союзу в рамках Програми партнерства ЄС та Світового банку в Європі та Центральній Азії та Програмного траст фонду за участю одного донора (Програма ЄС з реформування державного управління та фінансів (EURoPAF)) для реалізації Проекту зміцнення управління державними ресурсами.

Міністерство фінансів України (далі – МФУ) відповідає за реалізацію Частини В Проекту і, з метою посилення своєї спроможності щодо впровадження Проекту, залучає на умовах конкурсного відбору індивідуального консультанта – Консультанта з інформаційної кібербезпеки з підтримки документування (далі – Консультант) для реалізації організаційно-технічних заходів з розробки та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційній системі МФУ.

Консультаційні послуги (надалі - Послуги) передбачають надання МФУ допомоги в рамках етапів процесу розробки та створення комплексної системи захисту інформації (далі – КСЗІ) інформаційно-телекомунікаційної системи МФУ (далі - ІТС МФУ), з:

1) Проведення передпроектних досліджень середовищ функціонування ІТС МФУ;
2) Здійснення проектування КСЗІ ІТС МФУ в частині підготовки технічної документації;
3) Підготовка КСЗІ до введення в експлуатацію (не включає етап проведення державної експертизи).

Послуги надаватимуться в місці проживання Консультанта.

Очікується що Консультант буде працювати впродовж періоду з листопада 2020 року до березня 2021 року. Очікувані трудовитрати загалом не повинні перевищувати 120 робочих днів.

Консультант працюватиме в межах затвердженого Технічного завдання, яке додається.

МФУ запрошує правомочних фізичних осіб з – місцевих індивідуальних консультантів (надалі - Кандидати) висловити свою зацікавленість щодо надання Послуг у формі резюме (українською чи англійською мовами). Зацікавлені кандидати мають надати інформацію щодо відповідності своєї кваліфікації та досвіду для виконання Послуг.

Кандидати мають надати підтвердження у формі посилання на публічно підтверджену та доступну інформацію чи надання копій відповідних документів що засвідчують відповідний статус чи стан.

Кандидати можуть додавати будь-які інші додаткові матеріали, які можуть підтверджувати наявність заявленого кандидатом досвіду та кваліфікації.

Вимоги до кваліфікації зацікавлених кандидатів наступні.

Обов'язкові кваліфікаційні вимоги:

- вища технічна освіта;
- досвід роботи у сфері захисту інформації не менше п’яти років, з яких не менше 2 років впродовж останніх 5 років
- наявність свідоцтва про підвищення кваліфікації у сфері технічного та криптографічного захисту інформації не менше одного за кожним напрямком,
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ впродовж останніх 5 років не менше 3 реалізованих договорів/проектів
- Знання та наявність навичок практичного застосування основних сервісів Microsoft, мережевих сервісів (DNS, DHCP, VLAN, VPN);
- досвід роботи із засобами мережевої безпеки.
- вільне володіння письмовою та усною українською мовою.

Кваліфікаційні вимоги, які відповідають специфіці завдання та будуть прийматись як перевага:

- наявність сертифікату СПБІС (CISSP) (Сертифікований професіонал з безпеки інформаційних систем) або САІС (CISA) (Сертифікований аудитор інформаційних систем) або СМІС (CISM) (Сертифікований менеджер інформаційних систем);
- наявність сертифікату про успішне проходження тренінгу/навчального курсу з питань впровадження та використання вимог ISO / IEC 27001:2013 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» за напрямками Впроваджувач та/чи Аудитор
- досвід впровадження комплексних системи захисту інформації різних типів (АС1, АС2, АС3);
- наявність наукового ступеню за технічними науками
- наявність авторських патентів на розробки в галузі ТЗІ та КЗІ
- наявність ліцензії Державної служби спеціального зв’язку та захисту інформації України на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ для організацій державного сектору економіки

- володіння англійською мовою на рівні опрацювання технічної документації в сфері IT без словника.

Зацікавлені Кандидати мають звернути увагу на Розділ III, параграфи , 3.14,3.16, та 3.17, «Керівництва МБРР із закупівель для Позичальників інвестиційних проектів» (липень 2016 року, переглянуте в листопаді 2017 та серпні 2018 року) (далі – Керівництво із закупівель) що визначає політику Світового банку щодо конфлікту інтересів.

Відбір Консультанта здійснюватиметься за процедурою відбору індивідуальних консультантів (IC), за правилами встановленими у вищевказаному Керівництві.

Зацікавлені Кандидати можуть отримати додаткову інформацію за зазначеною нижче контактною інформацією з 10:00 до 18:00 окрім вихідних днів:

Контактна особа: Володимир Воротюк
Телефон: +38 044 206 5773, 380 50 4100340
Ел.пошта: vorotyuk@outlook.com

Висловлення зацікавленості слід направляти електронною поштою за наведеною нижче адресою до 17:00 (за місцевим часом) 4 листопада 2020 року.

Міністерство фінансів України
До уваги: Ігоря Шевлякова, Керівника експертної групи з європейської інтеграції Директорату стратегічного планування та європейської інтеграції.
Тема листа – "Висловлення зацікавленості - MF-IC-14, **Консультант з інформаційної кібербезпеки з підтримки документування** "
Ел.пошта: shevliakov@minfin.gov.ua, обов'язкова копія vorotyuk@outlook.com.

Додаток до REoI №MF-IC-14

ТЕХНІЧНЕ ЗАВДАННЯ

на надання консультаційних послуг:

Консультант з інформаційної кібербезпеки з підтримки документування

(Індивідуальний консультант)

Номер закупівлі №: MF-IC-14

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Уряд України отримав фінансування з боку Міжнародного банку реконструкції та розвитку (далі – Світовий банк), який виступає адміністратором коштів гранту, наданого Європейською комісією від імені Європейського Союзу (далі – Донор) в рамках Програми партнерства ЄС та Світового банку в Європі та Центральній Азії та Програмного траст фонду за участю одного донора (Програма ЄС з реформування державного управління та фінансів (EURoPAF)) у розмірі 3 030 661 євро (далі – Грант) для реалізації Проекту зміцнення управління державними ресурсами (далі – Проект). Цей Проект складається з двох частин: Частини А «Зміцнення управління людськими ресурсами на державній службі» та Частини В «Підтримка впровадження Стратегії управління державними фінансами».

Частина В Проекту, обсягом 1 110 618 євро, передбачає підтримку заходів для реалізації Стратегії реформування системи управління державними фінансами на 2017-2020 роки та визначення майбутніх потреб в інвестиціях в ІКТ системи в сфері управління державними фінансами шляхом проведення ІКТ аудиту; модернізації існуючого ІКТ обладнання для підтримки безперервної роботи МФУ; посилення спроможності ІКТ систем та ін.

Для досягнення мети одним із головних завдань Стратегії реформи управління державними фінансами є широке запровадження надійних ІТ-рішень та автоматизація існуючих процесів у сфері управління державними фінансами, з метою мінімізації людського впливу та пов’язаних із цим корупційних викликів.

Міністерство фінансів України (далі – МФУ) відповідає за реалізацію Частини В Проекту і, з метою посилення своєї спроможності щодо впровадження Проекту, залучає на умовах конкурсного відбору індивідуального консультанта – Консультанта з інформаційної кібербезпеки з підтримки документування (далі – Консультант) для реалізації організаційно-технічних заходів з розробки та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційній системі МФУ.

2. ОПИС ПРОБЛЕМИ

На сьогодні в Україні, кожний державний орган та підприємство повинні забезпечувати максимальну автоматизацію процесів своєї життєдіяльності, оперативну взаємодію та обмін інформацією в процесі прийняття управлінських рішень.

Залежність організації від інформаційних систем, які забезпечують її життєдіяльність, стає причиною серйозних ризиків щодо забезпечення захисту інформаційних ресурсів, які

обробляються їхніми засобами. Відмова в роботі такої інформаційної системи або несанкціоноване втручання в її роботу може мати катастрофічні наслідки як для організації, так і для країни в цілому. Тому одночасно з впровадженням інформаційних систем (далі – ІС) велика увага приділяється їх безпеці, відмовостійкості та захисту інформації, яка циркулює в системах.

Інформаційно-телекомунікаційна система МФУ (далі – ІТС) представляє собою сервісно-орієнтовану програмно-апаратну платформу впровадження та виконання типізованих прикладних інформаційних сервісів, які реалізуються на єдиній програмно-апаратній платформі, підтримують єдину технологію обробки інформації та забезпечують механізми реалізації положень єдиної політики безпеки затвердженої МФУ.

Програмно-апаратна платформа ІТС реалізує стратегію єдиної інтеграційної системи, що об'єднує в собі технології та програмні засоби, які дозволяють забезпечувати функціонально замкнуту та самодостатню систему обробки даних в рамках створюваних (впроваджуємих) прикладних сервісів (автоматизованих систем) з підтримкою визначених фіксованих (для усіх систем ІТС) типів об'єктів захисту, суб'єктів доступу (груп і ролей користувачів) та базовими умовами експлуатації.

Відповідно до ст. 6 Закону України «Про доступ до публічної інформації» та ст. 21 Закону України «Про інформацію» до інформації, яка обробляється засобами інформаційних систем органів державної влади та яка зберігається в державних реєстрах, висуваються вимоги щодо забезпечення її конфіденційності, цілісності та доступності в процесі її обробки.

Таким чином, з метою забезпечення політики безпеки ІТС у відповідності до вимог чинного законодавства України та виключення або мінімізації збитку, спричиненому несанкціонованим доступом до інформаційних ресурсів повинна бути створена комплексна система захисту інформації (далі – КСЗІ) з підтвердженою відповідністю відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

В цілому комплексну систему захисту інформації можна визначити як комплекс організаційних та інженерно-технічних заходів, правових та законодавчих норм, а також фізичних, програмно-апаратних та програмних засобів захисту інформації. Необхідність застосування комплексних систем захисту інформації встановлено законодавством України, а порядок їх створення визначений Адміністрацією Держспецзв'язку.

В процесі розробки та управління комплексною системою захисту інформації ІТС повинен застосовуватися інтегрований підхід впровадження на усіх представлених рівнях архітектури ІТС, що передбачає:

- Реалізацію єдиної політики захисту інформації, яка підтверджується атестатом відповідності на КСЗІ ІТС та розробка регламентів і порядків нарощування функціонального та програмно-апаратного забезпечення в процесі масштабування і модернізації інфраструктури та обчислювальних ресурсів ІТС;
- Скорочення термінів впровадження додаткових інформаційних систем (функціональних сервісів) та нарощування автоматизованих робочих місць

користувачів сервісів (далі – АРМ) за рахунок застосування типових проектних рішень забезпечення послуг безпеки та погодження із Адміністрацією Держспецзв'язку України порядків їх впровадження (комплекс механізмів захисту впроваджуваного сервісу (АРМ) включається до системи керування безпекою ІТС);

- Можливість динамічного нарощування обчислювальних потужностей ІТС та середовища користувачів без необхідності додаткової/повторної експертизи;
- Зменшення забезпечення та супроводження системи, за рахунок уникнення дублювання типових документів (моделі, проекти, інструкції, настанови тощо) та організаційно-технічних заходів безпеки (аудит, оновлення тощо).
- Зменшення видатків пов'язаних із проведенням додаткових експертиз.

КСЗІ ІТС розробляється згідно типового порядку створення КСЗІ в АС (НД ТЗІ 3.7-003), з урахуванням інтегрованого підходу щодо реалізації складових її архітектури.

Метою створення комплексної системи захисту інформації ІТС є забезпечення захисту інформації, яка обробляється засобами ІТС, шляхом запобігання та протидії несанкціонованому доступу, розголошенню, спотворенню та втратам при її обробці і передачі. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування компонентів ІТС. Комплексна система захисту інформації є невід'ємною складовою частиною ІТС.

КСЗІ є комплексом програмних і технічних засобів та організаційних заходів спрямованих на забезпечення встановленого рівня захисту інформації відповідно до умов середовищ експлуатації ІТС та вимог забезпечення основних характеристик безпеки, визначених політикою безпеки ІТС та організації-розпорядника. КСЗІ ІТС призначена для реалізації положень політики безпеки інформації в частині:

- ідентифікації та автентифікації користувачів ІТС під час доступу та використання об'єктів захисту;
- керування авторизованими користувачами та розподілу повноважень щодо використання інформаційних та програмних ресурсів ІТС;
- забезпечення конфіденційності та цілісності інформації, яка циркулює в ІТС та/або передається між її компонентами;
- забезпечення ідентифікації та автентифікації вузлів ІТС під час сеансу взаємодії;
- забезпечення конфіденційності та цілісності інформації, яка надається зовнішнім користувачам/системам;
- забезпечення ідентифікації та автентифікації вузлів зовнішніх систем під час сеансу взаємодії;
- забезпечення конфіденційності, цілісності та доступності технологічної інформації щодо функціонування системи;
- забезпечення доступності інформації, яка циркулює в ІТС, для авторизованих користувачів та процесів;
- реєстрації та обробки всіх подій в ІТС, які мають відношення до безпеки інформації;
- реалізації моніторингу актуального стану безпеки та працездатності компонентів ІТС;

– управління всіма механізмами безпеки через відповідний інтерфейс адміністрування, який повинен бути доступним тільки уповноваженому персоналу.

3. МЕТА ЗАВДАННЯ

Метою завдання є надання послуг МФУ в рамках етапів процесу розробки та створення КСЗІ ІТС МФУ, з:

- Проведення передпроектних досліджень середовищ функціонування ІТС МФУ;
- Здійснення проектування КСЗІ ІТС МФУ в частині підготовки технічної документації;
- Підготовка КСЗІ до введення в експлуатацію (не включає етап проведення державної експертизи).

4. ОБСЯГ ПОСЛУГ ТА ЗАВДАННЯ

Консультант має виконувати наступні завдання відповідно до наступних етапів:

4.1 *На етапі* передпроектних досліджень середовищ функціонування ІТС МФУ консультант повинен:

4.1.1. Здійснити обстеження середовищ функціонування ІТС МФУ (зокрема обчислювальної системи ІТС, інформаційного та фізичного середовища, середовища користувачів, визначити загальну структурну схему і склад (перелік і склад обладнання, технічних і програмних засобів, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо), види і характеристики каналів зв'язку, особливості взаємодії окремих компонентів.

4.1.2. Провести аналіз вразливостей програмно-апаратного забезпечення реалізації компонентів ІТС, середовищ експлуатації та технології обробки інформації відповідно до визначених рівнів представлення архітектури, з використанням загальнодоступних джерел та програмно-технічної документації розробників.

4.1.3. Підготувати документи за результатами аналізу, як визначено в п.п.1 Розділу 5 цього Завдання.

4.1.4. Підготувати та подати відповідний звіт з проведення передпроектного обстеження і вносити до нього зміни, у разі необхідності.

На етапі здійснення проектування КСЗІ ІТС МФУ консультант повинен

4.2

4.2.1 Виконати розробку загальних проектних рішень, необхідних для реалізації вимог ТЗ відповідно до сценаріїв реалізації загроз, рішень щодо структури КСЗІ ІТС, алгоритмів функціонування та умов використання засобів захисту, в рамках яких визначити:

- функції КСЗІ в цілому та функції її окремих складових частин;
- склад КЗЗ;
- детальну схему компонентів КСЗІ та схему взаємодії її складових частин;

- алгоритми функціонування та умови використання засобів захисту;
- рішення щодо архітектури КЗЗ, з урахуванням затверджених рівнів та інтегрованих компонентів системи, та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації;

склад та технічні вимоги до засобів КЗІ.

4.2.2. Підготувати документи за результатами аналізу, як визначено в п.п.2 Розділу 5 цього Завдання.

4.2.3. Підготувати та подати відповідний звіт зі створення проектної документації техноробочого проекту КСЗІ і вносити до нього зміни, якщо необхідно

4.3 На етапі підготовки КСЗІ до введення в експлуатацію підготувати документи, як визначено в п.3 Розділу 5 цього Завдання, а саме:

4.3.1 Розробити проекти організаційно-розпорядчої документації з розробки та впровадження КСЗІ ІТС (накази, розпорядження, протоколи, акти тощо).

4.3.2 Розробити комплекти експлуатаційної документації та технологічних інструкцій, відповідно до затверджених рішень проектів КЗЗ та організаційної структури.

4.3.3 Підготувати навчальні матеріали для проведення інструктажу користувачів ІТС МФУ в частині дотримання вимог КСЗІ ІТС (принцип проведення – інтерактивний курс тривалістю не більше 4 годин).

4.3.4 Провести попередні випробування КСЗІ ІТС МФУ та підготувати відповідний протокол за результатами попередніх випробувань.

4.3.5 Підготувати та подати відповідний звіт з підготовки КСЗІ до введення в експлуатацію і вносити до нього зміни, якщо необхідно

5. РЕЗУЛЬТАТИ ДІЯЛЬНОСТІ КОНСУЛЬТАНТА ТА ГРАФІК НАДАННЯ МАТЕРІАЛІВ

Консультант має підготувати та надати МФУ наступні результати[1]:

No.	**Результат**	**Строк надання** *(з дати укладання договору з консультантом)*
1	Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ, який включає: • модель загроз та модель порушника для центру обробки даних (далі – ЦОД) ІТС МФУ; • модель загроз та модель порушника для системи оперативно-технічного управління (далі – СОТУ) ІТС МФУ;	Впродовж 90 робочих днів

[1] Наповнення результатів та строк виконання завдання може бути уточнено під час контрактних переговорів з консультантом, відповідно до запропонованої методології надання послуг.

	• модель загроз та модель порушника для підсистеми прикладних сервісів (далі – ППС) ІТС; • модель загроз та модель порушника для автоматизованих робочих місць (далі – АРМ) • положення про службу захисту інформації в ІТС; • звіт та проект акту обстеження середовищ функціонування ІТС; • політика безпеки інформації;	
2	Звіт з підготовки технічного проекту КСЗІ ІТС МФУ, який включає: а) Проектну документацію техноробочого проекту КСЗІ: • опис комплексу технічних засобів забезпечення захисту інформації центрального сегменту (далі – ЦС) ІТС МФУ; • опис комплексу криптографічних засобів забезпечення захисту інформації; • настанова з інсталяції засобів КЗЗ та генерування базових параметрів політики безпеки компонентів ЦОД ІТС МФУ; • настанова з інсталяції засобів КЗІ та генерування базових параметрів політики безпеки компонентів СОТУ ІТС МФУ 1) Пояснювальна записка до технічного проекту. 2) Проект ОТР КСЗІ локального користувача – працівника Міністерства фінансів України 3) Проект ОТР КСЗІ АРМ віддаленого користувача – працівника Міністерства фінансів України та/або підпорядкованих структур 4) Проект ОТР КСЗІ АРМ віддаленого користувача – користувача зовнішніх інформаційних систем, які здійснюють взаємодію із ППС ІТС 5) Настанова з інсталяції засобів КЗЗ та генерування базових параметрів політики безпеки ОТР КСЗІ АРМ локального користувача – працівника Міністерства фінансів України 6) Настанова з інсталяції засобів КЗЗ та генерування базових параметрів політики безпеки ОТР КСЗІ АРМ віддаленого користувача –	Впродовж 100 робочих днів

	працівника Міністерства фінансів України та/або підпорядкованих структур 7) Настанова з інсталяції засобів КЗЗ та генерування базових параметрів політики безпеки ОТР КСЗІ автоматизованого робочого місця віддаленого користувача – користувача зовнішніх інформаційних систем. б) Нормативно розпорядчу документацію КСЗІ: • інструкція системного адміністратора; • інструкція технічного адміністратора; • інструкція з експлуатації ІТС в частині захисту інформації; • порядок модернізації КЗЗ; • порядок керування конфігурацією КЗЗ; • технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ: - інструкція про порядок резервування та відновлення інформації; - інструкція про порядок оперативного відновлення функціонування; - інструкція про організацію контролю за функціонуванням КСЗІ; - інструкція про порядок забезпечення антивірусного захисту; - інструкція про порядок підключення автоматизованих робочих місць адміністраторів та респондентів.	
3	Звіт з підготовки до введення в експлуатацію КСЗІ ІТС МФУ, який включає: а) документацію щодо проведених випробувань КСЗІ: • програма та методика попередніх випробувань КСЗІ в ІТС; • протокол попередніх випробувань КСЗІ в ІТС. б) організаційно-розпорядчу документація КСЗІ: • проект наказу про призначення служби захисту інформації; • проект наказу про проведення обстеження середовищ функціонування ІТС; • проект наказу про проведення попередніх випробувань та дослідної експлуатації КСЗІ ІТС;	Впродовж 110 робочих днів

	• проект акту приймання у дослідну експлуатацію КСЗІ ІТС; • навчальні матеріали щодо інструктажу користувачів ІТС МФУ в частині дотримання вимог КСЗІ ІТС • проект акту завершення дослідної експлуатації КСЗІ ІТС.	

6. КООРДИНАЦІЯ, ПІДЗВІТНІСТЬ ТА ЗВІТУВАННЯ

Консультант працює під керівництвом Координатора Проекту від МФУ та є йому підзвітним. Всі документи, які готуються Консультантом, в подальшому можуть бути включенні до пакету документів, який буде затверджений на рівні нормативно-правового акту МФУ.

Консультант має координувати свою роботу з координатором МФУ з ІТ-питань в частині розробки узгоджених рішень для відпрацювання та побудови концептуальної моделі, закладеної в проекті Стратегії розвитку інформаційних технологій Міністерства фінансів України на 2020-2022 роки та надання вихідної інформації щодо виконання завдань представникам МФУ.

Консультант в рамках оперативної взаємодії погоджує свою роботу з Провідним консультантом з інформаційної кібербезпеки (Індивідуальний консультант) та співпрацює з профільним підрозділом МФУ, відповідальним за впровадження функцій з захисту інформації.

Провідний консультант з інформаційної кібербезпеки (Індивідуальний консультант) уповноважений щодо Консультанта:

- контролює дотримання строків та якості підготовки всіх звітних документів Консультанта;
- надає коментарі (у разі їх наявності) до документації, що додається до звітності Консультанта, та перевіряє врахування таких коментарів.

Консультант готує та надає МФУ наступні звіти:

- Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ;

- Звіт з підготовки технічного проекту КСЗІ ІТС МФУ;

- Звіт з підготовки до введення в експлуатацію КСЗІ ІТС МФУ.

1. Консультант надає МФУ Звіт з проведення передпроектного обстеження середовищ функціонування ІТС МФУ не пізніше терміну встановленого для результату № 1 в розділі. 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:
    - інформація про перший етап виконання робіт згідно з переліком документів визначених в п.1 розділу 5 цього Технічного завдання;
    - проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;

- загальна інформація про готовність всього комплекту документів зазначених в п.1 розділу 5 цього Технічного завдання;
- інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату № 1 в п. 5 цього Технічного завдання.

2. Консультант надає МФУ Звіт з підготовки техноробочого проекту КСЗІ ІТС МФУ не пізніше терміну встановленого для результату № 2 в розділі 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:
   - загальна інформація про другий етап виконання робіт
   - проектну документацію техноробочого проекту КСЗІ відповідно до переліку документів визначених в п. 2 розділу 5 цього Технічного завдання;
   - проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;
   - загальну інформація про готовність всього комплекту документів зазначених в п 2 розділу 5 цього Технічного завдання;
   - інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату №. 2 п. 5 цього Технічного завдання.

3. Консультант надає МФУ Звіт за результатами введення в експлуатацію КСЗІ ІТС МФУ не пізніше терміну встановленого для результату № 3 розділу 5 цього Технічного завдання. Звіт готується за результатами виконання завдань та повинен включати наступну інформацію:
   - інформація про готовність комплекту документів зазначених в розділі 5 цього Технічного завдання результат № 3.
   - проблемні питання, які Консультант вбачає як перешкоди вчасного та якісного надання послуг та пропоновані заходи щодо їх усунення;
   - інша інформація на розсуд Консультанта.

До Звіту додається підготовлена Консультантом документація, визначена для результату № 3 в розділі 5 цього Технічного завдання.

4. Вимоги до звітів

Всі звіти готуються українською мовою. Будь-які додаткові документи до них подаються мовою оригіналу.

Всю звітність Консультант подає наступним чином:

- Консультант подає звітні документи в електронному вигляді для розгляду та надання коментарів МФУ на адресу _____ (звіти мають бути підписані, відскановані в форматі pdf файлу та відправлений з електронної адреси Консультанта зазначеної в п. 5 нижче). Супроводжуюча документація повинна

бути у форматі MS Word, MS Excel або MS PowerPoint, чи іншому форматі прийнятному для МФУ, залежно від типу документу.

- у випадку погодження МФУ наданих Консультантом документів в електронній формі, Консультант має подати відповідні документи в паперовій формі в 2-х екземплярах підписаних Консультантом. Паперові версії направляються поштою за наступною адресою: *04071, м. Київ, вул. Межигірська, буд. 11, до уваги Ігоря Шевлякова*.

У випадку, якщо звіт Консультанта посилається на раніше підготовлену інформацію або документи, такі документи повинні бути додані до звіту. Структура та форма звітних документів, зазначених у Розділі 5 цього Технічного завдання, визначається вимогами нормативних документів системи технічного захисту інформації.

5. Розгляд та затвердження Звітів

МФУ розглядає подану звітність та затверджує або надає зауваження протягом 10 робочих днів з дати отримання відповідного звіту за результатами роботи. Зауваження до звітів викладаються письмово та направляються Консультанту засобами електронного зв'язку на електронну поштову скриньку _____ з повідомленням про доставку відповідного повідомлення. Консультант впродовж доби після отримання зауважень від МФУ, повідомляє про отримання відповідних зауважень та строк їх врахування. Поправки (зауваження) МФУ до відповідних звітів повинні бути враховані Консультантом та відповідний оновлений звіт має бути наданий МФУ не пізніше 5 робочих днів з дати їх надходження на вказану електронну скриньку Консультанта.

У випадку відсутності надання МФУ зауважень впродовж вказаного терміну, такі звіти вважаються прийнятими.

7. РЕСУРСИ ЗАМОВНИКА

МФУ забезпечує Консультанта:

i) всіма відповідними документами і даними, які не мають грифу обмеження доступу або не віднесені до конфіденційної інформації;

ii) доступом до приміщення МФУ;

iii) у випадку необхідності контакту з організаціями, що входять до структури державного управління фінансами, МФУ забезпечує здійснення такого контакту для Консультанта.

8. ОБМЕЖЕННЯ

В Договорі з Консультантом застосовується стандартне положення щодо Конфлікту інтересів. Крім цього, всі матеріали, створені під час надання послуг за договором, залишаються власністю МФУ і можуть використовуватись лише з офіційного письмового дозволу МФУ.

До початку надання послуг Консультант разом з МФУ готує заяву про конфіденційність, де бере на себе зобов'язання не розголошувати конфіденційну інформацію, яку може отримати під час виконання завдання. Положення заяви про конфіденційність повинні відповідати вимогам чинного законодавства України.

9. МІСЦЕ, ТРИВАЛІСТЬ, УМОВИ ПРАЦІ ТА ВИНАГОРОДА

Очікується що Консультант буде працювати впродовж періоду з листопада 2020 року до березня 2021 року. Очікувані трудовитрати загалом не повинні перевищувати 120 робочих днів. Завдання передбачає роботу Консультанта, як в місці його проживання.

Обсяг винагороди буде визначений в результаті переговорів з обраною особою та проводитиметься на основі наданих результатів робіт, що оформлюються відповідними звітами.

Консультант відповідальний за всі видатки, які він несе у зв'язку з наданням послуг, зокрема наступними, але не обмежуючись ними: проживання в місці надання послуг, переклади, витрати на зв'язок.

Відбір Консультанта буде проводитись відповідно до вимог «Керівництва МБРР із закупівель для Позичальників інвестиційних проектів» (липень 2016 року, переглянуте в листопаді 2017 та серпні 2018 року).

10. ВИМОГИ ДО ОСВІТИ ТА КВАЛІФІКАЦІЇ

Консультант повинен відповідати наступним кваліфікаційним вимогам:

Обов'язкова кваліфікація Консультанта:

- вища технічна освіта;
- досвід роботи у сфері захисту інформації не менше п'яти років, з яких не менше 2 років впродовж останніх 5 років
- наявність свідоцтва про підвищення кваліфікації у сфері технічного та криптографічного захисту інформації не менше одного за кожним напрямком,
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ впродовж останніх 5 років не менше 3 реалізованих договорів/проектів
- Знання та наявність навичок практичного застосування основних сервісів Microsoft, мережевих сервісів (DNS, DHCP, VLAN, VPN);
- досвід роботи із засобами мережевої безпеки.
- вільне володіння письмовою та усною українською мовою.

Додаткові кваліфікаційні вимоги, які відповідають специфіці завдання та будуть прийматись як перевага

Відповідність Консультанта наступним кваліфікаційним вимогам буде розглядатись Замовником, як перевага:

- наявність сертифікату СПБІС (CISSP) (Сертифікований професіонал з безпеки інформаційних систем) або САІС (CISA) (Сертифікований аудитор інформаційних систем) або СМІС (CISM) (Сертифікований менеджер інформаційних систем);
- наявність сертифікату про успішне проходження тренінгу/навчального курсу з питань впровадження та використання вимог ISO / IEC 27001:2013 «Інформаційні

технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» за напрямками Впроваджувач та/чи Аудитор

- досвід впровадження комплексних системи захисту інформації різних типів (АС1, АС2, АС3);
- наявність наукового ступеню за технічними науками
- наявність авторських патентів на розробки в галузі ТЗІ та КЗІ
- наявність ліцензії Державної служби спеціального зв'язку та захисту інформації України на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації
- досвід побудови КСЗІ та підготовки документів для проведення державних експертиз в галузі ТЗІ для організацій державного сектору економіки
- володіння англійською мовою на рівні опрацювання технічної документації в сфері ІТ без словника

Кандидати мають надати підтвердження у формі посилання на публічно підтверджену та доступну інформацію чи надання копій відповідних документів що засвідчують відповідний статус чи стан.