Додаток 1

1. ЗАДАНІ ВИМОГИ ДО ПРЕДМЕТА ЗАКУПІВЛІ

1.1. ЗАГАЛЬНІ ВИМОГИ

1.1.1. Предмет закупівлі

Предметом закупівлі є консультаційні послуги щодо проведення діагностики цільового профілю безпеки інформації в інформаційно-комунікаційній системі, власником якої є Міністерство оборони України. Послуги закуповуються та надаються на користь розпорядника системи – Центру інновацій та розвитку оборонних технологій

Послуги надаються з метою:

Здійснення повторної щорічної оцінки повноти та якості впровадження контролів безпеки, передбачених відповідним цільовим профілем безпеки інформації системи;

зниження ймовірності виникнення інцидентів інформаційної безпеки та витоку інформації, зокрема персональної та службової інформації, обробка якої здійснюється в системі;

забезпечення незалежної оцінки впровадження контролів безпеки, що стане основою для подання повторної декларації/ здійснення державної авторизації з безпеки системи.

1.1.2. Вимоги щодо дотримання вимог нормативних документів

При наданні послуги необхідно враховувати положення таких нормативних документів:

Основні:

Постанова Кабінету Міністрів України № 627 від 30 травня 2024 р. “Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації”;

Постанова Кабінету Міністрів України № 712 від 18 червня 2025 р. “Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем”;

Наказ Адміністрації Держспецзв’язку від 24.06.2024 № 317 “Про визначення Базового профілю безпеки інформації”;

Наказ Адміністрації Держспецзв’язку від 02.07.2025 № 419 «Про затвердження базового профілю безпеки системи, де обробляється службова інформація»;

Наказ Адміністрації Держспецзв’язку від 10.07.2024 № 354 “Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації";

NIST SP 800-53a Rev. 5 "Assessing Security and Privacy Controls in Information Systems and Organizations" та NIST SP 800-171a Rev.3 "Assessing Security Requirements for Controlled Unclassified Information"

Допоміжні:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

ДСТУ ISO/IEC 27001:2023 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT);

ДСТУ 7731:2015 "Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)";

НД ТЗІ 3.6-005-21 "Порядок категоріювання безпеки інформаційної системи та інформації";

НД ТЗІ 3.6-006-21 "Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем";

НД ТЗІ 3.6-007-21 "Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем";

НД ТЗІ 2.3-025-21 "Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем";

НД ТЗІ 2.6-004-21 "Порядок авторизації безпеки інформаційних систем";

НД ТЗІ 3.6-008-21 "Порядок моніторингу безпеки інформаційних систем";

FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems. 2004;

FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems, 2006;

NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 1.1, April 2018;

NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012;

NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018;

NIST Special Publication 800-39. Managing Information Security Risk:

Organization, Mission, and Information System View, 2011;

NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020;

NIST Special Publication 800-64. Rev.2. Security Considerations in the System Development Life Cycle, 2008;

NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011;

NIST Special Publication 800-160 Vol. 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2018;

NIST Special Publication 800-160 Vol. 2. Developing Cyber Resilient Systems: A Systems Security Engineering Approach, 2019.

**Вищенаведений перелік є невиключним, орієнтовним, та може уточнюватись в ході надання послуг.*

1.1.3. Кваліфікаційні вимоги

1.1.3.1 Вимоги щодо ліцензій та дозволів:

Надавач послуг зобов’язаний мати чинну ліцензію на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, в частині оцінювання захищеності інформації, що не становить державної таємниці.

1.1.3.2 Інші вимоги

- Надавач послуг зобов’язаний мати спеціалістів, які сертифіковані за міжнародниим стандартами (CISA – не менше 3, CISM – не менше 1, OSCP – не менеше 1, NIST Cybersecurity Framework Lead Implementer – не менше 2)
- Не менше 6 спеціалістів Надавача послуг мають попередній досвід проведення діагностики (оцінювання) систем згідно з постановою Кабінету Міністрів України № 627 від 30 травня 2024 р. “Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації”
- Не менше 6 спеціалістів надавача мають досвід проведення діагностики цільового профілю безпеки інформації в інформаційно-комунікаційній системі, власником якої є Міністерство оборони України

1.1.3.3 Субпідряд. Залучення третіх осіб

Учасник може залучати субпідрядників лише за попередньою письмовою згодою Замовника.

Наступні роботи не можуть передаватися на субпідряд: управління проєктом, планування та методологія оцінювання, формування та підписання підсумкового звіту з оцінювання.

Допускається залучення технічних експертів лише під керівництвом та контролем Учасника.

Будь-яка заміна чи залучення додаткового субпідрядника під час виконання договору допускається лише за письмовою згодою Замовника. Замовник має право обґрунтовано відмовити або вимагати заміни субпідрядника.

1.1.4. Порядок надання послуги

Окремі заходи різних етапів можуть виконуватись паралельно.

Всі етапи мають відбуватися в тісній взаємодії з особовим складом Центру інновацій та розвитку оборонних технологій.

1.1.4.1. Етап 1 — Первинна діагностика

1. Ознайомлення з об'єктом аналізу, збір і вивчення Цільового Профілю Безпеки (ЦПБ) та базових матеріалів. Аналіз впроваджених заходів захисту щодо вимог ЦПБ.
2. Розробка методики діагностики, та діагностика впроваджених заходів захисту відповідно до наданого ЦПБ
3. Надання попереднього звіту з висновками, наявними прогалинами та загальними рекомендаціями по їх усуненню. Звіт має містити опис методики діагностики для кожного заходу захисту ЦПБ, результати діагностики.

1.1.4.2. Етап 2 — Фінальна діагностика

1. Проведення повторної діагностики в розрізі прогалин та невідповідностей які були виявлені на Етапі 1.
2. Збір та систематизація доказової бази (артефактів) для кожного із впроваджених заходів захисту.
3. Надання фінального деталізованого звіту щодо реалізації заходів захисту інформації та структурованого пакету інформації (артефактів), які дозволяють пересвідчитися в повноті проведеної діагностики (посилання на внутріші норматвні документи, елементи конфігураційних файлів, скріншоти налаштувань тощо)
4. Підготовка та надання скороченого звіту, для вищого керівництва.

1.1.5. Вимоги до процедури звітування та оцінки відповідності наданих послуг

Виконавець інформує Замовника про виконання заходів передбачених на всіх етапах надання послуг та готовність до передачі напрацювань (документів).

Для кожного реалізованого заходу захисту відповідно до надого ЦПБ Виконавець передає Замовнику пакет інформації, що підтверджує факт та стан впровадження. Пакет містить релевантні артефакти: затверджені політики, накази, процедури (або зміни до них), витяги з конфігурацій і параметрів систем, журнали подій, скріншоти налаштувань, реєстри доступів, записи про зміни, акти, службові записки та інші матеріали.

Підсумкова звітність із зазначенням результатів виконання заходів за етапом та акт виконаних робіт за результатами виконання відповідного етапу надається Виконавцем в термін зазначений в плані надання послуг за договором.

1.2. ВИМОГИ ДО НАДАННЯ ПОСЛУГИ

Виконавець самостійно визначає та забезпечує інструменти, необхідні для надання Послуги.

Виконавець виконує всі дії у тісній взаємодії з фахівцями Центру інновацій та розвитку оборонних технологій.

Виконавець може залучати власних спеціалістів виключно за погодженням із Центром інновацій та розвитку оборонних технологій, в т.ч. за умови успішного проходження спеціальних перевірок.

Заборонено використання неліцензійного, піратського програмного забезпечення, а також програмного забезпечення, правовласником якого є організації, пов'язані з російською федерацією.

Для забезпечення надання Послуги Виконавцеві надається обмежений та контрольований гостьовий доступ до інструментів спільної роботи та комунікації у відповідності до внутрішніх правил та процедур Замовника.

Сторони можуть узгоджувати зміни у форматі звітних документів, зокрема у разі зміни законодавства.

1.3. ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА КОНФІДЕНЦІЙНОСТІ

Вимоги щодо забезпечення охорони державної таємниці під час надання Послуги не висуваються.

Виконавець повинний забезпечити конфіденційність інформації, яка була отримана під час надання Послуги.

У випадку залучення Виконавцем до надання Послуги третьої сторони Виконавець зобов'язаний забезпечити дотримання третьою стороною всіх вимог щодо забезпечення конфіденційності наданої інформації.

Залучення третіх сторін, які не є резидентам України, забороняється.

1.4. ТЕРМІН НАДАННЯ ПОСЛУГИ

Термін надання послуги не повинен перевищувати 3 (трьох) місяців з дати підписання договору.

1.5. АДРЕСА НАДАННЯ ПОСЛУГИ

Адреса надання послуг: м. Київ, проспект Повітряних Сил, 6 (конкретна адреса буде надана під час організації надання послуг)*.

Виходячи з міркувань безпеки, з урахуванням того, що послуги надаються на користь Центру інновацій та розвитку оборонних технологій, який є органом військового управління, вся необхідна інформація для виконання договору надається Переможцю відповідної процедури після підписання договору щодо нерозголошення конфіденційної інформації).