Request for Proposals (RFP) /
Запит на надання пропозиції (Запит)

USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (USAID Cybersecurity)
Проєкт USAID "Кібербезпека критично важливої інфраструктури України" (Проєкт USAID Кібербезпека)

REQ-KYI-24-0209

Provision of services for diagnostics of the cybersecurity level of critical infrastructure objects according to the NIST Cybersecurity Framework 2.0 for the USAID Cybersecurity Activity
Надання послуг з діагностування рівня кібербезпеки об'єктів критичної інфраструктури згідно NIST Cybersecurity Framework 2.0 для Проєкту USAID Кібербезпека

Issued by: DAI Global, LLC
Видано: DAI Global, LLC

Issue Date: September 17, 2024
Дата: 17 вересня 2024

WARNING: Prospective Offerors who have received this document from a source other than DAI, should immediately contact UkraineCCI_Procurement@dai.com and provide their name and mailing address in order that amendments to the RFP or other communications can be sent directly to them. Any prospective Offeror who fails to register their interest assumes complete responsibility in the event that they do not receive communications prior to the closing date. Any amendments to this solicitation will be issued and posted by email.

ПОПЕРЕДЖЕННЯ: Потенційні Учасники тендеру, які отримали цей документ з джерела іншого, ніж компанія «DAI», повинні негайно звернутися до UkraineCCI_Procurement@dai.com та вказати назву та адресу своєї компанії, щоб прямо на цю адресу їм можна було надсилати зміни до цього Запиту або інші повідомлення. Будь-який потенційний Учасник тендеру, який таким чином не виявить свою зацікавленість, бере на себе повну відповідальність у разі неотримання повідомлень до кінцевого терміну подання пропозиції. Будь-які зміни до цього Запиту надсилатимутися електронною поштою.

DAI
Shaping a more livable world.

Table of Contents/Зміст

Synopsis of the Request for Proposals (RFP)
Стислий огляд запиту на надання пропозиції (Запит)

1. RFP No. REQ-KYI-24-0209

2. Issue date: September 17, 2024

3. Title

Critical Infrastructure Cybersecurity Incident Preparedness Assessment (CICIPA) for the State of Archival Service of Ukraine.
Procurement of services to conduct a diagnosis of the cybersecurity system of the State of Archival Service of Ukraine to assess the level of cyber maturity in accordance with the requirements of the NIST Cybersecurity Framework and provide recommendations for improving the state of cyber readiness under USAID Cybersecurity Activity.

4. E-mail address for submission of Proposals

Proposals should be submitted to UkraineCCI_Proposals@dai.com.

5. Deadline for Receipt of Questions
October 03, 2024, Kyiv, 2 p.m. Ukraine Time to the e-mail address UkraineCCI_Procurement@dai.com
Questions and requests for clarifications – and the responses thereto will be circulated in writing to all RFP recipients who have indicated interest in responding to this RFP. Both questions and answers will be distributed, without identification of the inquirer(s), to all prospective Offerors who are on record as having received this RFP. In addition, questions and answers will be posted publicly on the same platform where the RFP is posted.

6. Deadline for receipt of Proposals

October 10, 2024 4 p.m., Kyiv, Ukraine Time to the e-mail address UkraineCCI_Proposals@dai.com

PLEASE NOTE THAT THE E-MAIL ADDRESS FOR THE RECEIPT OF QUESTIONS AND THE E-MAIL ADDRESS FOR RECEIPT OF PROPOSALS ARE DIFFERENT

7. Point of contact

UkraineCCI_Procurement@dai.com

1. Запит № REQ-KYI-24-0209

2. Дата надання запиту: 17 вересня 2024

3. Назва

Закупівля послуг діагностування поточного рівня кібербезпеки для Державної архівної служби України.

Закупівля послуг діагностування поточного рівня кібербезпеки Державної архівної служби України та надання рекомендацій для покращення та посилення рівня захисту від кібер атак в рамках Проєкту USAID Кібербезпека.

4. Електронна адреса для подання пропозицій

Пропозиції мають подаватись на адресу:
UkraineCCI_Proposals@dai.com

5. Кінцевий термін отримання запитань
14.00 за місцевим київським часом в Україні **03 жовтня 2024 року**, на адресу: UkraineCCI_Procurement@dai.com
Питання та запити на роз'яснення - і відповіді на них будуть надані в письмовій формі для всіх одержувачів Запиту на надання пропозиції, які вказали зацікавленість у відповіді на нього. Питання і відповіді будуть поширені, без ідентифікації запитувача (ів), для всіх потенційних пропозицій. Крім того, питання та відповіді будуть розміщені публічно на тій же платформі, де розміщений Запит на надання попозицій

6. Кінцевий термін отримання пропозицій

16.00 за місцевим київським часом в Україні **10 жовтня 2024 року** на адресу: UkraineCCI_Proposals@dai.com

ЗВЕРНІТЬ УВАГУ, ЩО АДРЕСА ЕЛЕКТРОНОЇ ПОШТИ ДЛЯ ОТРИМАННЯ ЗАПИТАНЬ ТА АДРЕСА ЕЛЕКТРОНОЇ ПОШТИ ДЛЯ ОТРИМАННЯ ПРОПОЗИЦІЙ ВІДРІЗНЯЮТЬСЯ

7. Адреса для запитів

UkraineCCI_Procurement@dai.com

8. Anticipated Award Type

Firm Fixed Price Purchase Order

9. Basis for Award

An award will be made based on the **Trade Off Method**. The award will be issued to an Offeror whose proposal is deemed responsible and reasonable and who provides the best value to DAI and its client using a combination of technical and cost/price factors.
To be considered for award, Offerors must meet the requirements identified in Section "Determination of Responsibility".

DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful Performance or delivery of quality goods and equipment. DAI does not tolerate corruption, bribery, collusion or conflicts of interest. Any requests for payment or favors by DAI employees should be reported as soon as possible to ethics@dai.com or by visiting www.dai.ethicspoint.com. Further, any attempts by an offeror or subcontractor to offer inducements to a DAI employee to influence a decision will not be tolerated and will be grounds for disqualification, termination and possible debarment.

8. Очікуваний вид контракту

Договір на закупівлю із фіксованою ціною

9. Підстава для укладення контракту

Рішення про укладання контракту буде прийматись на основі **методу порівняльного аналізу**. Контракт буде укладено з відповідальним та прийнятним Учасником тендеру, який подасть найкращу пропозицію DAI та клієнту компанії, використовуючи поєднання технічних та цінових/вартісних показників.
Для того, щоб прийняти участь у тендері, Учасники тендеру повинні відповідати вимогам, визначеним у Розділі «Визначення відповідальності».

DAI веде свою діяльність відповідно до найсуворіших етичних стандартів, щоб забезпечити чесність конкуренції, прийнятні ціни та успішне надання послуг або доставку якісних товарів та обладнання. DAI не терпить корупції, хабарництва, змови чи конфлікту інтересів. Про будь-які запити на оплату або послуги співробітників DAI слід якомога швидше повідомляти на ethics@dai.com або відвідавши www.dai.ethicspoint.com. Крім того, будь-які спроби контрактера чи субпідрядника запропонувати співробітникам DAI заохочення та вплинути на рішення не будуть допускатися і стануть підставою для дискваліфікації, припинення та можливого блокування.

Introduction and Purpose / Вступ та Мета

Purpose	**Мета**
The purpose of this RFP is to obtain proposals from suppliers that can provide services to USAID Cybersecurity Activity (the Activity) DAI Global LLC to carry out diagnostics for the **State of Archival Service of Ukraine as per the requirements included in the Scope of Work of this RFP.**	Метою цього запиту є отримання пропозицій від постачальників, які зможуть надати послуги для Проєкту USAID Кібербезпека (далі – Проєкт), який виконується DAI Global LLC, з діагностування поточного рівня кібербезпеки **Державної архівної служби України, згідно вимог, зазначених в Технічному завданні до цього Запиту.**
Issuing Office	**Офіс, що видає запит на надання пропозицій**
The Issuing Office and Point of Contact noted in the above synopsis are the sole points of contact at DAI for the purposes of this RFP. Any prospective Offeror who fails to communicate their interest with this office assumes complete responsibility if they do not receive direct correspondence and relevant information (amendments, answers to questions, etc.) before the closing date.	Офіс, що видає Запит на надання пропозицій, та Контактна особа, зазначена у стислому огляді вище, є єдиною контактною особою в компанії «DAI» для цілей цього Запиту на надання пропозицій. Будь-який потенційний Учасник тендеру, який не зареєстрував свою зацікавленість в цьому офісі, бере на себе повну відповідальність у випадку, якщо він не буде одержувати прямі повідомлення та відповідну інформацію (зміни, відповіді на запитання тощо) до дати закриття.
Type of Award Anticipated	**Очікуваний вид контракту**
A **Firm Fixed Price Purchase Order** is an award for a total firm fixed price for the provision of specific services, goods, or deliverables. It is not adjusted if the actual costs are higher or lower than the fixed price amount. Offerors are expected to include all direct and indirect costs into their total proposed price. Issuance of this RFP in no way obligates DAI to award a purchase order and Offerors will not be reimbursed for any costs associated with the preparation of their bid.	**Контракт із фіксованою ціною** – це винагорода за загальну фіксовану ціну, за надання конкретних послуг, товарів чи результатів, яка не коригується, якщо фактичні витрати вищі або нижчі за фіксовану ціну. Очікується, що учасники тендеру включатимуть усі прямі та непрямі витрати до загальної запропонованої ціни. Надання цього Запиту в жодному разі не зобов'язує компанію «DAI» укладати договір на закупівлю, і Учасникам тендеру не відшкодовуються будь-які витрати, пов'язані з підготовкою пропозиції.

General Instructions to Offeror/Загальні інструкції

General Instructions	Загальні інструкції
• "Offeror", "Subcontractor", and/or "Bidder" means a firm proposing the work under this RFP. "Offer" and/or "Proposal" means the package of documents the firm submits proposing how it will carry out the work.	• «Учасник тендеру» та/або «Субпідрядник» означає фірму, яка пропонує виконати роботи в рамках цього Запиту на надання пропозицій. «Пропозиція» означає пакет документів, які фірма подає, щоб запропонувати виконання робіт.
• Offerors wishing to respond to this RFP must submit proposals **in English** in accordance with the RFP instructions. Offerors are required to review all instructions and specifications contained in this RFP. Failure to do so will be at the Offeror's risk. If the solicitation is amended, then all terms and conditions not modified in the amendment shall remain unchanged.	• Учасники тендеру, які бажають відповісти на цей Запит на надання пропозицій, повинні подавати пропозиції **англійською** відповідно до інструкцій, вказаних у цьому документі. Учасники тендеру зобов'язані переглянути всі інструкції та технічні характеристики, що містяться в цьому Запиті на надання пропозицій. Ризики нездійснення цього несе Учасник тендеру. Якщо запрошення до надання пропозицій буде змінено, тоді всі положення та умови, які не були змінені, залишаться незмінними.
• Issuance of this RFP in no way obligates DAI to award a subcontract or purchase order. Offerors will not be reimbursed for any costs associated with the preparation or submission of their proposal. DAI shall in no case be responsible for liable for these costs.	• Оприлюднення цього Запиту на надання пропозицій жодним чином не зобов'язує компанію «DAI» укладати субконтракт або договір на закупівлю. Учасникам тендеру не будуть відшкодовуватися будь-які витрати, пов'язані з підготовкою або поданням їх пропозиції. За жодних обставин, компанія «DAI» не несе відповідальності за ці витрати.
• Proposals are due no later than **October 10, 2024, 4 p.m.**, Kyiv, Ukraine Time.	• Пропозиції мають бути подані **не пізніше 16:00** за місцевим київським часом в Україні **10 жовтня 2024 року.**
• Please note that Offerors shall submit complete proposals **in electronic form only** to UkraineCCI_Proposals@dai.com.	• Зверніть увагу, що пропозиції мають подаватися **лише в електронному вигляді** на електронну адресу UkraineCCI_Proposals@dai.com.
• Late offers will be rejected except under extraordinary circumstances at DAI's discretion.	• Пропозиції, подані пізніше, будуть відхилені, за винятком випадків надзвичайних обставин на розсуд компанії «DAI».
• The submission to DAI of a proposal in response to this RFP will constitute an offer and indicate the Offeror's agreement to the terms and conditions in this RFP and any attachments hereto. DAI reserves the right not to evaluate a non-responsive or incomplete proposal.	• Подання пропозиції компанії «DAI» у відповідь на цей Запит на надання пропозицій буде являти собою пропозицію та свідчитиме про згоду Учасника тендеру з положеннями та умовами, які містяться у цьому Запиті на надання пропозицій та будь-яких додатках до нього. Компанія «DAI» залишає за собою право не оцінювати невідповідну або неповну пропозицію.
• The RFP number and title shall be indicated ***in the subject line of e-mails.***	• ***У темі повідомлення електронною поштою*** мають бути зазначені номер Запиту та назву.
• Offerors shall sign, seal, and date their proposal cover letter. The Offeror shall submit this letter in .pdf format.	• Усі пропозиції повинні містити супровідний лист, що має дату, підпис та печатку Учасника тендеру. Учасник тендеру подає цей лист у форматі .pdf.

• Offerors shall complete **Attachment C**: Price Schedule. Offerors should indicate the total and all-inclusive price for services, roll them up, and distribute them across the listed deliverables in the USD or Hryvnia (UAH) Offerors shall be informed that all payments will be made in **local currency** as per the regulations of the cooperating country. If the contract is signed in dollars and the invoice is submitted in dollars, the program will pay the vendor in **local currency (hryvnias) using DAI's bank exchange rate on the transfer day.** • **Value Added Tax (VAT) shall not be included in the Price Schedule.** These services are eligible for VAT exemption based on the USAID Contract №72012120C00002 registered with the Cabinet of Ministers of Ukraine, having the registration card **№4464-24 of August 12, 2024**. • Each Offeror and any of its subsidiaries shall submit only one proposal.	• Учасники тендеру заповнюють **Додаток С:** Прайс-лист. Учасники тендеру повинні вказати загальну та всеосяжну ціну на послуги, загальну ціну та розподілити ціну по вказаних результатах в доларах США або гривні. Учасники тендеру повині бути проінформовані, що усі платежі здійснюватимуться **в місцевій валюті** згідно з законодавством України. Якщо договір буде підписано в доларах США, і рахунок-фактуру надано в доларах США, програма сплатить постачальнику **в місцевій валюті (гривнях) за банківським курсом банку Проєкту на день переказу.** • **Податок на додану вартість (ПДВ) не має бути зазначений у прайс-листі.** Ці послуги підлягають звільненню від оподаткування ПДВ відповідно до основного контракту компанії «DAI» з USAID №72012120C00002 зареєстрованим у Кабінеті Міністрів України, реєстраційна картка **№4464-24 від 12 серпня 2024 року**. • Кожен Учасник тендеру, та будь-які його дочірні компанії, може подати лише одну пропозицію.
Proposal Cover Letter	**Супровідний лист до пропозиції**
A cover letter shall be included with the proposal on the Offeror's company letterhead with a duly authorized signature and company stamp/seal using **Attachment B** as a template for the format. The cover letter shall include the following items: • The Offeror will certify a validity period of **60 calendar days** for the prices provided. • Acknowledge the solicitation amendments received, if applicable.	Пропозиція має включати супровідний лист на фірмовому бланку Учасника тендеру, скріплений підписом належним чином уповноваженої особи та штампом/печаткою компанії з використанням **Додатку В** в якості шаблонного формату. Супровідний лист повинен містити такі пункти: • Учасник тендеру повинен підтвердить період чинності запропонованих цін протягом **60 календарних днів**. • Підтвердження отримання тендерних правок, якщо застосовно.
Questions Regarding the RFP	**Запитання стосовно Запиту**
Each Offeror is responsible for very carefully reading and fully understanding the terms and conditions of this RFP. All communications regarding this solicitation must be submitted via e-mail to UkraineCCI_Procurement@dai.com no later than the date specified above. All questions received will be compiled and answered in writing and distributed to all interested Offerors. **Questions SHOULD NOT be submitted to UkraineCCI_Proposals@dai.com.** No questions will be answered by phone. Any verbal information received from a DAI or USAID Cybersecurity Activity employee or other entity shall	Кожен Учасник тендеру є відповідальним за дуже уважне прочитання цього Запиту та повне розуміння його умов. Усе спілкування стосовно цього Запиту має надсилатись електронною поштою на адресу: UkraineCCI_Procurement@dai.com не пізніше дати, зазначеної вище. Всі отримані запитання будуть зібрані, і відповіді на них будуть надіслані електронною поштою усім зацікавленим Учасникам тендеру. **Запитання НЕ МАЮТЬ подаватися за адресою UkraineCCI_Proposals@dai.com** Відповіді на будь-які запитання не будуть надані по телефону. Будь-яка вербальна інформація, отримана від працівника компанії «DAI», або Проєкту USAID

not be considered an official response to any question regarding this RFP.	Кібербезпека чи іншої організації, не вважається офіційною відповіддю на будь-яке запитання щодо цього Запиту на надання пропозицій.
Instructions for the Preparation of Technical Proposals	**Інструкції щодо підготовки технічних пропозицій**
Technical proposals shall be sent in a separate attachment from cost/price proposals and clearly labeled as **"VOLUME I: TECHNICAL PROPOSAL".** Technical proposals shall include the following contents: 1. A document in MS Word of approximately maximum 3-5 pages that responds to the evaluation sub-criteria "**Technical Approach**". Description of the proposed services which meet or exceed the stated technical specifications or scope of work. The proposal must show how the Offeror plans to complete the work (specific steps that will be taken to produce the outputs listed in attachments A and C) and describe an approach that demonstrates the achievement of timely and acceptable Performance of the work. In this section, the Offeror must also show an understanding of the services desired and how they intend to design a product that will satisfy their client. 2. **Management approach** – Description of the Offeror's staff who will be assigned to the project and their roles and responsibilities. The proposal should describe how the proposed team members have the necessary experience and capabilities to carry out the Technical Approach. This section should also include the Offeror's Approach to communicating with DAI as well as a timeline for delivering the required services. CVs and Certificates for each team member are mandatory to be provided. 3. **Past Performance** – Provide a list of at least three (3) recent awards of similar scope and duration. The information shall be supplied as a table and shall include the legal name and address of the organization for which services were performed, a description of work performed, the duration of the work and the value of the Contract, a description of any problems encountered and how it was resolved, and a current contact phone number of a responsible and knowledgeable representative of the organization. See Attachment G. 4. **Experience in addressing the needs stipulated under "Additional task to task B at the request of the OCI". Offerors to provide information related**	Технічні пропозиції повинні бути надіслані в окремому додатку окремо від цінової пропозиції і мають бути чітко марковані як **«ТОМ І: ТЕХНІЧНА ПРОПОЗИЦІЯ»**. Технічні пропозиції повинні містити такі положення: 1. Документ у MS Word, об'ємом приблизно 3-5 сторінок, який відповідає підкритеріям оцінки **«Технічний підхід»**. У пропозиції повинно бути показано, як Учасник тендеру планує завершити роботу (конкретні кроки, які будуть вжиті для отримання результатів, перелічених у Додатках А та С), та описано підхід, який демонструватиме забезпечення своєчасного та прийнятного виконання робіт. У цьому розділі Учасник тендеру повинен продемонструвати розуміння бажаних послуг та того, як вони мають намір створити продукт, який задовольнить їх клієнта. 2. **Управлінський підхід** – Опис персоналу Учасника тендеру, який буде закріплено за проектом, яка буде їх роль та відповідальність. У пропозиції слід описати, що запропоновані члени команди мають необхідний досвід та можливості для виконання Технічного підходу. Цей розділ повинен включати підхід Учасника щодо комунікації з DAI, а також графік надання необхідних послуг. Обов'язково потрібно надати Резюме для кожного члена команди та Сертифікати. 3. **Досвід роботи** – Надайте список щонайменше 3 (трьох) останніх контрактів аналогічного обсягу та тривалості. Інформація подається у вигляді таблиці і вона повинна містити юридичну назву та адресу організації, якій надавалися послуги, опис виконаних робіт, тривалість роботи та вартість контракту, опис будь-яких проблем, що виникали, і як вони були вирішені, а також дійсний контактний номер телефону відповідального та компетентного представника організації. Дивись Додаток G. 4. **Досвід для задоволення потреб, визначених у розділі «Додаткове завдання до завдання В на запит OCI». Учасники надають інформацію стосовно досвіду, своїх співробітників і завершених завдань.**

to the specific experience the company and its employees have and the tasks completed.	
Services Specified	**Визначення послуг**
For this RFP, DAI needs the services described in **Attachment A**.	У зв'язку з цим Запитом на надання пропозицій DAI потребує послуг, які описані в **Додатку А.**
Technical Evaluation Criteria	**Критерії технічної оцінки**
Each proposal will be evaluated and scored against the evaluation criteria and evaluation sub-criteria, which are stated in the table below. Cost/price proposals are not assigned points, but for overall evaluation purposes of this RFP, technical evaluation factors and cost/price, when combined, are considered significantly more important than cost/price factors alone.	Кожна пропозиція буде оцінюватися відповідно до критеріїв оцінки та субкритеріїв оцінки, які вказані в таблиці нижче. Цінові пропозиції не оцінюються за бальною системою, однак для цілей загальної оцінки цього Запиту на надання пропозицій, фактори технічної оцінки, вартості/ціни, при їх поєднанні вважаються значно більш важливими, ніж фактори вартості/ціни.
NOTE: The proposal will be evaluated and scored on technical aspects first. Only the price proposals of those Offerors that pass the minimum qualifying score of **70** points in the technical evaluation will advance to cost evaluation. Proposals not reaching this qualifying score in the technical evaluation will be considered non-competitive and will not be evaluated.	**ПРИМІТКА**: Пропозицію буде оцінено в першу чергу за технічні аспекти. Лише цінові пропозиції тих Учасників, які під час технічної оцінки набрали мінімальний кваліфікаційний бал у **70** балів, перейдуть до етапу оцінки вартості. Пропозиції, які не набрали цього кваліфікаційного балу в технічній оцінці, вважатимуться неконкурентоспроможними та не будуть оцінюватися.
Technical Competence as presented in the Technical Proposal with the possible 100 points in total made up as follows: Technical Competence – presented in the Technical Proposal (100 points in total) **Technical Approach** (30 points) **Management Approach** (25 points) **Past Performance** (25 points) **Additional task to Task B at the request of the OCI** (20 points)	Технічна компетентність, представлена в Технічній пропозиції, із 100 можливими загальними балами формується наступним чином: Технічна компетентність – представлена в технічній пропозиції (загалом 100 балів) **Технічний підхід** (30 балів) **Управлінський підхід** (25 балів) **Досвід роботи** (25 балів) **Додаткове завдання до завдання В на запит OCI** (20 балів)

Evaluation Criteria/ Критерії оцінки

Offerors shall provide a clear, specific, and concise technical proposal that covers both the conceptual and practical approaches and addresses the following in the order specified below:

Учасники тендеру повинні надати чітку, конкретну та стислу технічну пропозицію, яка охоплює як концептуальний, так і практичний підходи та стосується наступного у порядку, зазначеному нижче:

Evaluation Criteria/ Критерії оцінки		
Technical Approach / Технічний підхід	The proposal is expected to contain the full description of the technical approach and will be evaluated based on how well it addresses the task based on the requirements of the RFP, including: • a detailed methodological approach to conducting diagnostics and evaluating the current level of cybersecurity level according to the NIST Cybersecurity Framework 2.0; • clarity and comprehensibility of the procedure for determining the duration of work. • a methodology for developing recommendations and a roadmap for their implementation/consultation support for the object of critical infrastructure, • confirmed experience of work in the field of critical infrastructure cybersecurity for the same or similar activities. Пропозиції оцінюються, виходячи із відповідності запропонованих рішень на основі вимог викладених у запиті, включаючи: • детальний методологічний підхід до проведення діагностики, а також оцінювання поточного та цільового рівня кібербезпеки згідно NIST Cybersecurity Framework 2.0; • чіткість та зрозумілість процедури визначення тривалості виконання робіт; • методологія розробки рекомендацій, дорожньої карти їх впровадження та консультативної підтримки рецепієнта; • підтверджений досвід роботи в сфері кібербезпеки критичної інфраструктури.	30points / 30 балів
Client and Management Approach/ Клієнтський та Управлінський підхід	• List of qualified technical specialists assigned to support the Activity and respond to immediate requests. • Confirmed experience of the proposed personnel (qualifications, resume) in the field of conducting cyber security diagnostics of critical infrastructure objects with an indication of the projects in which the personnel participated (a list of relevant projects of each proposed specialist) Qualifications of team members must be confirmed by internationally recognized certificates, namely: • 5 points for meeting the minimum requirements (qualifications of at least 2 employees must be confirmed by internationally recognized certificates, such as: CISA, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, including at least one employee with the Certified NIST Cybersecurity Framework Lead Implementer certificate	25 points / 25 балів

	• additionally, 4 points for certified specialists with certificates: CISM, CISSP, Certified NIST Cybersecurity Framework Lead Auditor, CGEIT, CRISC. • Перелік кваліфікованих технічних спеціалістів наданих на підтримку Проєкту та для відповіді на термінові запити; • Підтверджений досвід запропонованого персоналу (кваліфікація, резюме) у сфері проведення діагностик кібербезпеки об'єктів критичної інфраструктури з вказанням проетків, де песронал приймав участь (перелік відповідних проектів кожного запропонованого спеціаліста) Кваліфікації членів команди має бути підтверджена міжнародно визнаними сертифікатами, а саме: • 5 балів за виконання мінімальних вимог (кваліфікація принаймні двох експертів має бути підтверджена міжнародно визнаними сертифікатами, такими як: CISA, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, у тому числі не менше одного співробітника з сертифікатом Certified NIST Cybersecurity Framework Lead Implementer) • додатково по 4 бали за наявність у команді спеціалістів, з сертифікатами: CISM, CISSP, Certified NIST Cybersecurity Framework Lead Auditor, CGEIT, CRISC.	
Past Performance / Досвід роботи	• Evidence that the company has experience in carrying out services similar to those outlined in the Scope of Work with USAID-funded projects or technical assistance programs in Ukraine? • Evidence that the company has experience in cybersecurity of critical infrastructure, developing policies and procedures, providing advice, conducting assessments for compliance with international and national cybersecurity standards, and determining the current and target maturity level of IT processes and cybersecurity processes? • Evidence that the company and its employees have the experience of at least three (3) similar projects in the field of information security during the last three years? • Prove that the company has experience in assessing information security at critical infrastructure facilities (such facilities are enterprises that meet the Law of Ukraine "On Critical Infrastructure" criteria or are officially included in the list of critical infrastructure facilities) • Підтвердження того, що компанія має досвід надання послуг, подібних до тих, що описані в Обсязі робіт з проектами або програмами технічної допомоги, що фінансуються USAID в Україні? • Підтвердження того, що компанія має досвід у сфері кібербезпеки критичної інфраструктури, розробки політик і процедур, надання консультацій, проведення оцінок на відповідність міжнародним і національним стандартам кібербезпеки та визначення поточного та цільового рівня зрілості IT-процесів і процесів кібербезпеки?	25 points / 25 балів

	• Підтвердження того, що компанія та її співробітники мають досвід не менше трьох (3) подібних проектів у сфері інформаційної безпеки протягом останніх трьох років? • Підтвердження, що компанія має досвід проведення оцінки інформаційної безпеки на об'єктах критичної інфраструктури (такими об'єктами є підприємства, які відповідають критеріям Закону України «Про критичну інфраструктуру» або офіційно включені до переліку об'єктів критичної інфраструктури)	
Experience to address the needs stipulated under "**Additional task to task B at the request of the OCI** " / Досвід для задоволення потреб, визначених у розділі «Додаткове завдання до завдання В на запит OCI»	• Does the company and its employees have specific experience and strategic competencies in performing the additional task? • How many similar tasks was implemented by the company at critical infrastructure facilities? • Чи має компанія та її співробітники специфічний досвід та стратегічні компетенції в виконанні додаткового завдання? Якщо так – надано перелік та підтвердження • Скільки подібних завдань було реалізовано компанією на обьєктах критичної інфраструктури?	20 points / 20 балів
Total Points / Загальна кількість балів		100 points/ 100 балів

Instructions for the Preparation of the Cost Proposal Інструкції щодо підготовки цінових пропозицій

Cost/Price Proposals	**Цінові пропозиції**
Cost/Price proposals shall be sent in a separate attachment from technical proposals and clearly labeled as **"VOLUME II: COST/PRICE PROPOSAL".** Provided in **Attachment C** is a template for the Price Schedule, for a fixed price for each service provided. Offerors shall complete the template and provide as much supporting details as possible to substantiate the proposed price. These services are eligible for VAT exemption based on USAID Contract 72012120C00002 registered with the Cabinet of Ministers of Ukraine, with registration card **#4464-24 dated August 12, 2024**.	Цінові пропозиції повинні бути надіслані в окремому додатку окремо від технічних пропозицій і мають бути чітко марковані як **«ТОМ II: ЦІНОВА ПРОПОЗИЦІЯ»**. У **Додатку С** надано шаблон Прайс-листу послуг. Учасники торгів заповнюють шаблон та вказують якомога більше деталей для обґрунтування запропонованої ціни. Ці послуги підлягають звільненню від оподаткування ПДВ відповідно до основного контракту компанії «DAI» з USAID №72012120C00002 зареєстрованим у Кабінеті Міністрів України, реєстраційна картка **№4464-24 від 12 серпня 2024 року**.
Basis for award	**Підстави для укладення контракту**
Best Value Determination	**Визначення кращої пропозиції**
DAI will review all proposals, and make an award based on the technical and cost evaluation criteria stated above and select the Offeror whose proposal provides the best value to DAI. DAI may also exclude an offer from consideration if it determines that an Offeror is "not responsible", i.e., that it does not have the management and financial capabilities required to perform the work required. Evaluation points will not be awarded for cost. The cost will primarily be evaluated for realism and reasonableness. DAI may award to a higher priced Offeror if a determination is made that the higher technical evaluation of that Offeror merits the additional cost/price. DAI may award to an Offeror without discussions. Therefore, the initial offer **must contain the Offeror's best price and technical terms.**	Компанія «DAI» проаналізує усі пропозиції та прийме рішення про укладення контракту на основі технічних критеріїв оцінки та вартісних критеріїв оцінки, зазначених вище, та відбере Учасника тендеру, який зробив найкращу пропозицію компанії «DAI». Компанія «DAI» також може відмовити у розгляді пропозиції, якщо вона встановить, що Учасник тендеру «не є відповідальним», тобто, що він не має управлінських та фінансових можливостей, необхідних для виконання відповідних робіт. Бали оцінки не нараховуються за вартість. Вартість оцінюється здебільшого на предмет реалістичності та обґрунтованості. Компанія «DAI» може прийняти рішення про укладення контракту з Учасником тендеру, який пропонує вищу ціну, якщо буде прийнято рішення про те, що більш висока технічна оцінка такого Учасника тендеру заслуговує на додаткову вартість/ціну. Компанія «DAI» може прийняти рішення про укладення контракту з Учасником тендеру без обговорення. Тому початкова пропозиція **повинна містити найкращу ціну та найкращі технічні умови Учасника тендеру.**
Determination of Responsibility	**Визначення відповідальності**
DAI will not enter into any type of agreement with an Offeror prior to ensuring the Offeror's responsibility. When assessing an Offeror's responsibility, the following factors are taken into consideration:	Компанія «DAI» не укладатиме жодних договорів з Учасником тендеру перш ніж не переконається у його відповідальності. При оцінюванні відповідальності Учасника тендеру беруться до уваги наступні фактори:

1. Provide copies of the required business licenses to operate in Ukraine (company registration documents, including documents from the tax authority about VAT status). 2. Evidence of a Unique Entity ID (SAM) number (explained below). 3. The source, origin, and nationality of the services are not from a Prohibited Country (explained below). 4. A brief overview of the company, including professional achievements. 5. The firm has had successful experience with related projects of similar scope and size **(Attachment G).**	1. Надання копій необхідних документів на здійснення діяльності в Україні (документи про реєстрацію компанії, включаючи документ від податкового органу про статус ПДВ). 2. Наявність номеру Unique Entity ID (SAM) (пояснюється нижче). 3. Джерело, походження та юрисдикційна приналежність послуг не з переліку Заборонених Країн (пояснення надані нижче). 4. Короткий огляд компанії, включаючи професійні досягнення. 5. Наявність успішного досвіду виконання робіт в аналогічних проектах у минулому **(Додаток G).**
Anticipated post-award Deliverables	**Очікувані результати після укладення контракту**
Upon awarding the contract, the deliverables and deadlines detailed in the table below will be submitted to DAI. The Offeror should detail proposed costs per deliverable in the Price Schedule. All deliverables must be submitted to and approved by DAI before payment is processed. See **Attachment C**: Price Schedule for more information on the anticipated post-award deliverables.	Після укладення контракту, результати робіт та кінцеві терміни виконання, детально описані в таблиці нижче, будуть подані компанії «DAI». Учасник тендеру повинен детально описати запропоновану вартість кожного результату робіт в Прайс-листі. Усі результати робіт мають бути подані та схвалені компанією «DAI» перед тим, як буде оформлена оплата. Дивитись **Додаток С**: Прайс-Лист для отримання додаткової інформації про очікувані результати після укладення контракту.
Inspection & Acceptance	**Перевірка та прийняття**
The designated DAI Project Manager will inspect from time to time the services being performed to determine whether the activities are being conducted in a satisfactory manner and ensure that all equipment or supplies are of acceptable quality and standards. The Selected Vendor shall be responsible for any countermeasures or corrective action within the scope of this RFP, which the DAI Chief of Party may require as a result of such inspection.	Визначений менеджер проєкту компанії «DAI» періодично перевірятиме послуги, які надаються, на предмет того, чи діяльність виконується задовільно та чи усе обладнання або поставки є прийнятними за якістю та стандартами. Обраний постачальник несе відповідальність за будь-які контрзаходи або коригувальні дії в межах цього Запиту на надання пропозицій, які можуть вимагатись Керівником проєкту компанії «DAI» за результатами такої перевірки.
Compliance with Terms and Conditions In addition to comply with the foresaid requirements, the Offerors are required to fully meet or exceed the significant not cost- related specifications: 1. Offeror must be registered in Ukraine as demonstrated by valid documents for operation in Ukraine (company registration documents, including document from the tax authority about VAT status).	**Відповідність вимогам** На додаток до відповідності вищезазначеним вимогам, Учасники повинні повністю відповідати або перевищувати нецінovим вимогам специфікації: 1. Учасник повинен бути зареєстрований в Україні, що підтверджується чинними документами для діяльності в Україні (реєстраційні документи

2. **Consent is required in writing** to receive payment for services solely by bank transferrin line with the terms stipulated in the signed Contract. 3. Offeror must have at least three (3) years of relevant experience in providing similar services (please fill in Attachment G: Past Performance). 4. The offeror must preferably have experience in performing such services to Ukrainian non-profit organizations or international non-governmental organizations. 5. Experience in providing services with a VAT exemption (preferably). 6. The Offeror must have adequate financial resources to perform the work within the required delivery schedule, as evidenced by the acceptance of DAI payment terms upon delivery and the acceptance of DAI as stated in the cover letter.	компанії, у тому числі документ від податкового органу про статус ПДВ). 2. **Письмова Згода** учасника на оплату послуг виключно у безготівковій формі на умовах, передбачених в підписаному Договорі. 3. Учасник повинен мати не менше трьох (3) років відповідного досвіду надання подібних послуг (будь ласка, заповніть Додаток G: Попередній досвід). 4. Бажано, щоб Учасник мав досвід надання подібних послуг українським некомерційним організаціям або міжнародним неурядовим організаціям. 5. Досвід надання послуг із звільненням від ПДВ (бажано). 6. Учасник повинен мати достатні фінансові ресурси для виконання робіт в межах необхідного графіку, що підтверджується прийняттям умов оплати DAI після доставки та прийняття DAI, як зазначено в супровідному листі.
General Terms and Conditions	**Загальні умови та положення**
Offeror shall be aware of the general terms and conditions for an award resulting from this RFP. The selected Offeror shall comply with all Representations and Certifications of Compliance listed in Attachment D.	Учасник тендеру має бути в курсі загальних умов для укладання контракту за результатами даного Запиту на надання пропозиції. Обраний учасник має відповідати усім Заявам та Підтвердженням про відповідність, зазначеним у Додатку D.
Prohibited Technology	**Заборонені Технології**
Bidders MUST NOT provide any goods and/or services that utilize telecommunications and video surveillance products from the following companies: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate thereof, in compliance with FAR 52.204-25.	Учасники торгів не повинні надавати будь -які товари та/або послуги, які використовують продукти телекомунікацій та відеоспостереження від таких компаній: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, або Dahua Technology Company, або будь -яка їх філія відповідно до FAR 52.204-25.
Geographic Code	**Географічний код**
Under the authorized geographic code for its contract DAI may only procure goods and services from the following countries. Geographic Code 110: Goods and services from the United States, the independent states of the former Soviet Union, or a developing country but excluding any country that is a prohibited source.	Відповідно дозволеного географічного коду для укладання договорів компанія «DAI» може закуповувати товари та послуги лише із наступних країн. Географічний код 110: Товари та послуги зі Сполучених Штатів, незалежних держав колишнього Радянського Союзу або країн, що розвиваються, але за винятком заборонених країн походження.

Geographic Code 935: Goods and services from the United States, the Cooperating Country, and developing countries other than advanced developing countries, but excluding any country that is a prohibited source. • DAI must verify the source, nationality, and origin, of goods and services and ensure (to the fullest extent possible) that DAI does not procure any services from prohibited countries listed by the Office of Foreign Assets Control (OFAC) as sanctioned countries. The current list of countries under comprehensive sanctions include Cuba, Iran, North Korea, Sudan, and Syria. DAI is prohibited from facilitating any transaction by a third party if that transaction would be prohibited if performed by DAI. • By submitting a proposal in response to this RFP, Offerors confirm that they are not violating the Source and Nationality requirements and that the services comply with the Geographic Code and the exclusions for prohibited countries.	Географічний код 935: Товари та послуги зі Сполучених Штатів, країн-партнерів та країн, що розвиваються, крім передових країн, що розвиваються, за винятком заборонених країн походження. • Компанія «DAI» зобов'язана перевірити джерело, юрисдикцію та походження товарів та послуг та (у максимально можливій мірі) переконатись, що жодні послуги не закуповуються із заборонених країн, які знаходяться у списку Управління контролю за іноземними активами (OFAC) як країни, на які розповсюджуються санкції. До поточного списку країн, на які розповсюджуються всеосяжні санкції, входять наступні країни: Куба, Іран, Північна Корея, Судан та Сирія. Компанії «DAI» забороняється сприяти будь-якій угоді третьої сторони, якщо така угода була б забороненою, якщо б її виконувала компанія «DAI». • Подаючи пропозицію у відповідь на цей Запит, Учасники тендеру підтверджують, що вони не порушують вимог до Джерела та Юрисдикції, і що послуги відповідають Географічному коду та виняткам щодо заборонених країн.
Unique Entity ID (SAM)	**Унікальний ідентифікатор організації (SAM)**
All U.S. and foreign organizations receiving first-tier subcontracts/ purchase orders with a value of $30,000 in equivalent and above are required to obtain a Unique Entity ID (SAM) number before signing the agreement. For those required to obtain a SAM ID number, you may see Instructions for Obtaining a SAM ID number (Attachment E) or contact the Activity Procurement Team.	Всі американські та іноземні організації, які отримують прямі субконтракти/договори на закупівлю на суму в еквіваленті 30 000 доларів США і вище, **повинні** отримати унікальний ідентифікатор організації (SAM) до підписання угоди. Для тих, кому потрібно отримати унікальний ідентифікатор організації (SAM), зверніться до Інструкції для отримання унікального ідентифікатору організації (SAM) (Дивись Додаток Е) або зверніться до Відділу Закупівель Проекту.
Anti-Corruption and Anti-Bribery Policy and Reporting Responsibilities	**Політика щодо боротьби з корупцією та боротьбою з хабарництвом та Відповідальної Звітності**
• DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful Performance or delivery of quality goods and equipment. **DAI does not tolerate the following acts of corruption:** • Any requests for a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special consideration by a DAI employee, Government official, or their representatives, to influence an award or approval decision.	DAI веде свою діяльність за найсуворішими етичними стандартами, щоб забезпечити чесність конкуренції, прийнятні ціни та успішне надання послуг або доставку якісних товарів та обладнання. **DAI не терпить таких корупційних дій:** • Будь -які запити на отримання хабара, віддачі, сприяння чи виплати у вигляді виплати, подарунка або спеціальної компенсації співробітнику DAI, урядовцю чи їх представникам впливають на рішення про нагородження або схвалення

• Any offer of a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special consideration by an offeror or subcontractor to influence an award or approval decision. • Any fraud, such as mis-stating or withholding information to benefit the offeror or subcontractor. • Any collusion or conflicts of interest in which a DAI employee, consultant, or representative has a business or personal relationship with a principal or owner of the offeror or subcontractor that may appear to unfairly favor the Offeror or subcontractor. Subcontractors must also avoid collusion or conflicts of interest in their procurements from vendors. Any such relationship must be disclosed immediately to DAI management for review and appropriate action, including possible exclusion from award. • These acts of corruption are not tolerated and may result in serious consequences, including termination of the award and possible suspension and debarment by the U.S. Government, excluding the Offeror or subcontractor from participating in future U.S. Government business. • Any attempted or actual corruption should be reported immediately by either the offeror, subcontractor or DAI staff to: • Toll-free Ethics and Compliance Anonymous Hotline at (U.S.) +1-503-597-4328 • Hotline website – www.DAI.ethicspoint.com, or E-mail to Ethics@DAI.com • USAID's Office of the Inspector General Hotline at hotline@usaid.gov. • By signing this proposal, the Offeror confirms adherence to this standard and ensures that no attempts shall be made to influence DAI or Government staff through bribes, gratuities, facilitation payments, kickbacks or fraud. The Offeror also acknowledges that violation of this policy may result in termination, repayment of funds disallowed by the corrupt actions and possible suspension and debarment by the U.S. Government.	• Будь -яка пропозиція хабара, відкату, сприяння чи виплати у вигляді платежу, подарунка або спеціальної винагороди від оферента чи субпідрядника для впливу на рішення про присудження чи схвалення. • Будь-яке шахрайство, таке як неправильне викладання або приховування інформації на користь оферента чи субпідрядника. • Будь -які змови або конфлікти інтересів, у яких працівник, консультант або представник DAI має ділові або особисті стосунки з принципалом або власником оферента чи субпідрядника, які можуть виявитися несправедливими у користь оферента чи субпідрядника. Субпідрядники також повинні уникати змов чи конфлікту інтересів у своїх закупівлях у постачальників. Будь -які такі відносини повинні бути негайно розкриті керівництву DAI для перегляду та прийняття відповідних заходів, включаючи можливе виключення з винагороди. • Ці корупційні дії не допускаються і можуть призвести до серйозних наслідків, включаючи припинення призначення винагороди та можливе призупинення та відмову уряду США, виключаючи оферента чи субпідрядника від участі у майбутніх бізнесах уряду США. • Будь-яка спроба чи фактична корупція повинна бути негайно повідомлена оферентом, субпідрядником або співробітниками DAI: • Безкоштовна анонімна гаряча лінія з питань етики та дотримання вимог за адресою (США) +1-503-597-4328 • Веб -сайт гарячої лінії - www.DAI.ethicspoint.com, або надіслати електронний лист на адресу Ethics@DAI.com • Офіс гарячої лінії Генерального інспектора USAID за адресою hotline@usaid.gov. • Підписуючи цю пропозицію, оферент підтверджує дотримання цього стандарту та гарантує, що не будуть зроблені спроби вплинути на DAI або урядовий персонал за допомогою хабарів, чайових, виплат за сприяння, відкату чи шахрайства. Учасник торгів також визнає, що порушення цієї політики може призвести до припинення, повернення коштів, заборонених корупційними діями, та можливого призупинення та заборони уряду США.
Offeror's Agreement with Terms and Conditions	**Згода Учасника тендеру з вимогами**

The completion of all RFP requirements in accordance with the instructions in this RFP and submission to DAI/Preparedness & Response of a quotation will constitute an offer and indicate the Offeror's agreement to the terms and conditions in this RFP and any attachments hereto. Issuance of this RFP in no way obligates DAI to award a purchase order, nor does it commit DAI to pay any costs incurred by the Offeror in preparing and submitting the proposal.	Виконання усіх вимог Запиту відповідно до інструкцій, зазначених в ньому, та подання пропозиції до відділу компанії DAI/Preparedness & Response складатиме пропозицію та засвідчуватиме згоду Учасника тендеру з вимогами цього Запиту та усіх додатків до нього. Надання цього Запиту в жодному разі не зобов'язує компанію «DAI» надавати договір на закупівлю або відшкодовувати Учасникам тендеру будь-які витрати, пов'язані з підготовкою та поданням пропозиції.
Attachments **See the list of official RFP attachments below.**	**Додатки** **Дивитись перелік офіційних додатків до цього документу нижче.**

Attachment A: SCOPE OF WORK/TERMS OF REFERENCE Додаток А: ТЕХНІЧНЕ ЗАВДАННЯ

The information below contains the technical requirements for the services. Offerors are requested to provide proposals containing the information below on official letterhead or official proposal format.
У таблиці нижче наведені технічні вимоги до послуг. Учасники тендеру повинні подати пропозиції, що містять відповідну інформацію на фірмовому бланку або відповідно до офіційного формату пропозиції.

Background	**Передумови**
The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity began in May 2020. USAID Cybersecurity for Critical Infrastructure in Ukraine Activity is a program funded by USAID and implemented by DAI. The overall goal of the Activity is to reduce and potentially eliminate cybersecurity vulnerabilities in CI and to transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. Over the five years of performance, the Activity will increase resilience and build capacity to prevent, detect, and respond to cyberattacks against CI in Ukraine. The Activity will accomplish this goal through the pursuit of three strategic objectives (SOs): • SO1: Create a safe and trusted environment to accelerate the development of people, processes, and technology in support of cybersecurity across CI sectors and assets in Ukraine. • SO2: Strengthen Ukraine as a sovereign nation built on a secure, protected, and dynamic economy, supported by a talented pool of human capital. • SO3: Stimulate demand for and supply of Ukrainian cybersecurity solutions and service providers to empower, equip, and finance cybersecurity entrepreneurs and businesses. The Activity is organized into three components. Activity tasks are highly interdependent and mutually reinforcing.	Проєкт USAID «Кібербезпека критично важливої інфраструктури України» (далі – Проєкт) почав свою двяльність в травні 2020 року. Проєкт USAID «Кібербезпека критично важливої інфраструктури України» фінансується USAID та реалізується DAI. Кінцева мета Проєкту –зменшення та потенційне усунення вразливостей кібербезпеки та перетворення України на проактивного лідера кібербезпеки. Протягом п’яти років Проєкт зміцнюватиме стійкість і розвиватиме спроможність запобігати, виявляти й боротися з кібератаками, націленими на критичну інфраструктуру (далі – КІ) України. Діяльність досягне цієї мети шляхом досягнення трьох стратегічних цілей: **Компонент 1**: Створення безпечного та надійного середовища для прискорення розвитку людей, процесів та технологій на підтримку кібербезпеки у секторах та активах в Україні. **Компонент 2**: Зміцнення України як суверенної держави, побудованій на безпечній, захищеній та динамічній економіці, підтриманій талановитим пулом людського капіталу. **Компонент 3:** Стимулювання попиту та пропозиції українських рішень та постачальників послуг з кібербезпеки для розширення можливостей, оснащення та фінансування підприємців та бізнесу з кібербезпеки. Діяльність організована трьома складовими. Завдання діяльності взаємозалежні і взаємно підсилені.
Context	**Контекст**
The Activity provides assistance to critical infrastructure objects in the energy and other sectors (hereinafter - OCI - within the meaning of the Law of Ukraine "On Critical Infrastructure" or officially included in the list of critical	Проект надає допомогу об’єктам критичної інфраструктури в енергетичному та інших секторах (далі – ОКІ – у розумінні Закону України «Про критичну інфраструктуру» або офіційно включені до

infrastructure objects) in strengthening their resistance to cybersecurity incidents. At the request of OCI, the Activity plans to conduct diagnostics of their cybersecurity systems. The result of the diagnosis will be an assessment of the current level of maturity of the OCI. The diagnosis is carried out in accordance with the NIST Cybersecurity Framework 2.0, and based on the results, recommendations will be developed to improve the cyber resilience of the organization in accordance with the NIST Cybersecurity Framework 2.0. The results of the diagnostic will also establish a basis for measuring the progress of strengthening the cyber resilience of the OCI after the implementation of the recommendations provided after the diagnosis	переліку об'єктів критичної інфраструктури) у посиленні їх стійкості до інцидентів кібербезпеки. На запит ОКІ Проект планує проведення діагностування кібербезпеки їх систем. Результатом діагностування буде оцінка поточного рівня зрілості ОКІ. Діагностування здійснюється у відповідності до NIST Cybersecurity Framework2.0 , а за результатами будуть розроблені рекомендації щодо підвищення кіберстійкості організації відповідно до NIST Cybersecurity Framework 2.0. Результати діагностування також встановлять основу для вимірювання прогресу посилення кіберстійкості ОКІ після впровадження рекомендацій, наданих після діагностування.
Objectives	**Цілі**
The overall goal of the task is to conduct a diagnosis of the cybersecurity system of OCI to assess the level of cyber maturity in accordance with the requirements of the NIST Cybersecurity Framework 2.0 and provide recommendations for improving the state of cyber readiness	Загальна мета завдання полягає в тому, щоб провести діагностування системи кібербезпеки ОКІ для оцінки рівня кіберзрілості відповідно до вимог NIST Cybersecurity Framework 2.0 та надати рекомендації щодо покращення стану кіберготовності
Tasks	**Задачі**
Carrying out diagnostic of the State of Archival Service of Ukraine (see Appendix H) (next – Object of critical infrastructure, OCI) cybersecurity systems, which will include the following steps performed in accordance with the NIST Cybersecurity Framework 2.0: a. Assessment of the current level of OCI cybersecurity maturity according to the NIST Cybersecurity Framework 2.0. The evaluation report must contain a list and description of the Recipient's key information systems and resources. b. Defining OCI target maturity levels according to the NIST Cybersecurity Framework 2.0. Development of recommendations for the transition from the current level to the target level of maturity. Recommendations should contain a list of necessary policies and processes of information (cyber) security, calculation of essential resources, definition of personnel competencies, and organizational structure. Based on the recommendations, a high-level design High-Level Design, (HLD) of the technical architecture of cyber security and an operational cyber security model should also be formed. HLD and operating model requirements:	Проведення діагностуваня системи кібербезпеки Державної архівної служби України (див. Додаток Н) (далі – Об'єкт критичної інфраструктури, ОКІ), що буде включати в себе наступні крокі виконані відповідно до NIST Cybersecurity Framework 2.0: a. Оцінювання поточного рівня зрілості кібербезпеки ОКІ відповідно до NIST Cybersecurity Framework 2.0. Звіт з оцінки повинен містити перелік та опис ключових інформаційних систем та ресурсів Реципієнта. b. Визначення цільового рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework 2.0 Розробка рекомендацій щодо переходу від поточного рівня до цільового рівня зрілості. Рекомендації повинні містити перелік необхідних політик та процесів інформаційної (кібер) безпеки, підрахунок необхідних ресурсів, визначення компетенцій персоналу, організаційну структуру. На основі рекомендацій повинні також бути сформовані високорівневий проект (High-Level Design, HLD) технічної архітектури кібербезпеки та

1) The HLD document is based on technical controls (software and hardware solutions) and requirements for it:
   i. A minimum of 2 manufacturers for each technical solution;
   ii. Contain prices in the Global Price List of manufacturers and without VAT.
   iii. The list of products must be submitted as a full-fledged Bill of Material (expanded specification indicating all components of the solution).
2) Structure of HLD:
   i. A list of projects for the implementation of technical controls of cyber security and related digital infrastructures (if necessary) and the purpose of each of them. The goal should be specific and clear and correspond to the actual technological content of the project.
   ii. General description and issues of the Project(s) of item 2(i)
   iii. Basic technical requirements for defined design solutions with quantitative and qualitative requirements.
   iv. High-level technological design (visualization of system components, relationships between them, and other data that help the reader get a reliable idea of the project).
   v. The composition of the technical solution (at least two specifications in the form of a Bill of Material).
   vi. Comparison table of technical solutions.
   vii. Implementation requirements (components and resource assessment).
3) Operating model and requirements for it:
   i. The operational model consists of policies, processes, organizational structure, key performance indicators (KPI), personnel, corporate governance structure
   ii. The operational model should contain technical personnel and an approximate description of their functional duties and responsibilities (taking into account the proposed design technical solutions)
   iii. The cost of implementing the operational model, namely - policies, processes, organizational structure, KPI, personnel, and corporate governance structure.

Additional task to task B at the request of the OCI: drafts of 10 information security policies

1. **Network security policy**

операційної моделі кібербезпеки. Вимоги до HLD та операційної моделі:

1) Документ HLD опирається на технічні контролі (програмні на апаратні рішення) та вимоги до нього:
   i. Мінімум 2 виробника на кожне технічне рішення;
   ii. Містити ціни в Global Price List виробників та без ПДВ.
   iii. Перелік продуктів повинен бути поданий у вигляді повноцінного Bill of Material (розгоргнута специфікація із зазначенням усіх складових рішення).
2) Структура HLD:
   i. Перелік проектів впровадження технічних контролів кібербезпеки та супутніх цифрових інфраструктур (якщо є потреба) та мета кожного із них. Мета має бути конкретною, чіткою та відповідати реальному технологічному змісту проекту.
   ii. Загальний опис та проблематика Проекту(-ів) пункту 2.i
   iii. Базові технічні вимоги до визначених проектних рішень з кількісними та якісними вимогами.
   iv. Високорівневий технологічний дизайн (візуалізація компонентів системи, взаємозв'язків між ними, інші дані, що допомагають читачу отримати достовірне уявлення про проект).
   v. Склад технічного рішення (мінімум дві специфікації у вигляді Bill of Material).
   vi. Порівняльна таблиця технічних рішень.
   vii. Вимоги до впровадження (складові та ресурсна оцінка).
3) Операційна модель та вимоги до неї:
   i. Операційна модель складається з: політик, процесів, організаційної структуру, ключових показників ефективності (КПЕ) персоналу, структури корпоративного управління.
   ii. Операційна модель повинна містити технічний персонал та орієнтовний опис його функціональних обов'язків та відповідальностей (бажано із урахуванням пропонованих проектних технічних рішень).
   iii. Вартість впровадження операційної моделі, а саме - політик, процесів, організаційної структуру, КПЕ, персоналу, структури корпоративного управління.

Protect your Network from unauthorized access, attacks, and other threats by implementing firewalls, intrusion detection systems (IDS), and other tools.

2. **Risk management policy**

Assessment, identification, and management of information security risks to reduce the likelihood of their occurrence and impact on the organization.

3. **Incident management policy**

Define the process of detecting, documenting, responding to, and eliminating security incidents to minimize their impact.

4. **Malware protection policy**

Prevent the penetration and spread of malicious software through the introduction of antivirus solutions and other security tools.

5. **Access control policy**

Defining access rights to information resources based on the roles and responsibilities of employees, in order to restrict access to sensitive information.

6. **Backup and restore policy**

Regularly create backups of critical data and systems with plans to restore it in case of loss or damage.

7. **Data privacy policy**

Protection of personal and confidential information from unauthorized access, disclosure or abuse.

8. **Physical premises security policy**

Protect the organization's physical resources and premises through access control, video surveillance, and other security measures.

9. **Password policy**

Set requirements for the complexity, length, frequency of changes, and password protection to ensure secure access to systems and data.

10. **Training and awareness policy**

Raising employees' awareness of information security threats and methods of preventing them through training programs and trainings.

Development of a roadmap for the implementation of the developed recommendations for 2 months and 3 years.

The roadmap must contain a list of actions that OCI should provide to achieve the target maturity level with a detailed description of each action and required resources (material, time, human).

c. Ten days of advisory support will be provided to OCI in the implementation process by OCI of developed recommendations, which will include, but not be limited to, consultation on adaptation and

Додаткове задача до завдання В за запитом ОКІ: проекти 10 політик інформаційної безпеки

1. **Політика безпеки мережі**

Захист мережі від несанкціонованого доступу, атак та інших загроз шляхом впровадження міжмережевих екранів, систем виявлення вторгнень (СВВ) та інших засобів.

2. **Політика управління ризиками**

Оцінка, ідентифікація та управління ризиками інформаційної безпеки для зменшення ймовірності їх виникнення та впливу на організацію.

3. **Політика управління інцидентами**

Визначення процесу виявлення, документування, реагування та усунення інцидентів безпеки для мінімізації їх впливу.

4. **Політика захисту від шкідливого ПЗ**

Запобігання проникненню та поширенню шкідливого програмного забезпечення через впровадження антивірусних рішень та інших засобів захисту.

5. **Політика управління доступом**

Визначення прав доступу до інформаційних ресурсів на основі ролей і відповідальностей співробітників, з метою обмеження доступу до чутливої інформації.

6. **Політика резервного копіювання та відновлення**

Регулярне створення резервних копій критичних даних і систем з планами для їх відновлення у разі втрати або пошкодження

7. **Політика конфіденційності даних**

Захист особистої та конфіденційної інформації від несанкціонованого доступу, розголошення або зловживання.

8. **Політика безпеки фізичних приміщень**

Захист фізичних ресурсів та приміщень організації шляхом контролю доступу, відеоспостереження та інших заходів безпеки.

9. **Політика паролів**

Встановлення вимог до складності, довжини, частоти зміни та захисту паролів для забезпечення безпеки доступу до систем і даних.

10. **Політика навчання та обізнаності**

Підвищення рівня обізнаності співробітників про загрози інформаційної безпеки та методи їх запобігання через навчальні програми та тренінги.

verification of procedures and policies and equipment settings. d. Development of a report on the implementation progress of the recommendations provided by the OCI. e. Evaluation of the maturity level of OCI's cybersecurity systems according to NIST Cybersecurity Framework 2.0 after 2 months from the date of receipt of recommendations by OCI.	Розробка дорожньої карти реалізації розроблених рекомендацій на 2 місяці та 3 роки. Дорожня карта повинна містити список заходів та їх пріорітизації, що має вжити ОКІ для досягнення цільового рівня зрілості з детальним описом кожного з них та визначеними для їх впровадження необхідних ресурсів (матеріальних, часових, людських). c. Надання десяти днів консультативної підтримки ОКІ в процесі впровадження ОКІ наданих рекомендацій, що буде включати в себе, але не обмежуючись: консультації по адаптації та верифікації процедур та політик та налаштувань обладнання. d. Розробка звіту про хід виконання рекомендацій наданих ОКІ. e. Оцінювання рівня зрілості систем кібербезпеки ОКІ відповідно до NIST Cybersecurity Framework 2.0 через 2 місяці з дати отримання ОКІ рекомендацій.

Deliverables schedule (assessment works are carried out within the framework of one project but separately for each of the critical infrastructure objects)		**Графік надання результатів (роботи з оцінювання проводяться в рамках одного проекту, але для кожного з об' єктів критичної інфраструктури - окремо)**	
Initial Stage: Signing of the Non-Disclosure Agreement (NDA) between OCI and the Contractor	20 working days after signing the Contract between the Activity and the provider	**Підготовчий етап:** Підписання договору про нерозголошення (НДА) між ОКІ та Підрядником	20 робочих днів з моменту підписання Договору між Проєктом та Підрядником
Task A Report: Assessment of the current OCI cybersecurity maturity level according to the NIST Cybersecurity Framework 2.0	30 working days after signing the NDA	**Звіт про завдання А:** Оцінка рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework 2.0	30 робочих днів з моменту підписання НДА
Task B Report: Determination of the OCI target maturity level according to NIST Cybersecurity Framework 2.0 Recommendations for transitioning from the current to the target level. The roadmap for the implementation of the developed recommendations for a period of 2 months and 3 years	40 working days after the completion of Task A	**Звіт про завдання В:** Визначення цільового рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework 2.0 Рекомендації щодо переходу від поточного рівня до цільового рівня зрілості. Дорожня карта впровадження розроблених рекомендацій на 2 місяці та 3 роки	40 робочих днів після виконання завдання А

Task C - D Report: The progress of each month of implementation of the recommendations by the recipient	45 working days after completion of Task B (the report shall capture the work completed under task C and D)	**Звіт по Завданню C та D**: Хід виконання рекомендацій реципієнтом за кожен місяць	45 робочих днів після виконання Завдання B (у звіті має бути відображено роботу, виконану за завданнями C та D)
Task E Report: Reassessment of the current cybersecurity maturity level according to the NIST Cybersecurity Framework 2.0	20 working days after the completion of Task D	Звіт про завдання E: повторна оцінка рівня зрілості кібербезпеки відповідно до NIST Cybersecurity Framework 2.0	20 робочих днів після виконання Завдання D

Minimum qualifications, skills, and experience	**Мінімальна кваліфікація, навички та досвід**
1. The provider must be registered and provide auditing, assessment, and consulting services in the field of cybersecurity in Ukraine within the last 3 years; 2. Employees of the provider must have experience in conducting at least 3 similar information security diagnostic projects during the last 3 years; 3. The qualifications of at least 2 of the supplier's employees must be confirmed by internationally recognized certificates, such as: CISA, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, including at least one employee with the Certified NIST Cybersecurity Framework Lead Implementer certificate; 4. Confirmed experience of the proposed personnel (qualifications, resume) in the field of conducting cyber security diagnostics of critical infrastructure objects with an indication of the projects in which the personnel participated (a list of relevant projects of each proposed specialist)	1. Постачальник має бути зареєстровий та надавати послуги з аудиту, оцінювання та консультування в сфері кібербезпеки в Україні протягом останніх 3 років; 2. Співробітники постачальника повинні мати досвід у проведенні не менше 3 подібних проектів діагностування інформаційної безпеки протягом останніх 3 років; 3. Кваліфікація принаймні 2 експертів має бути підтверджена міжнародно визнаними сертифікатами, такими як: CISA, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, у тому числі не менше одного співробітника з сертифікатом Certified NIST Cybersecurity Framework Lead Implementer; 4. Підтверджений досвід запропонованого персоналу (кваліфікація, резюме) у сфері проведення діагностик кібербезпеки об’єктів критичної інфраструктури з вказанням проектів, де персонал приймав участь (перелік відповідних проектів кожного запропонованого спеціаліста)

DIAGNOSTIC STRATEGY	**СТРАТЕГІЯ ДІАГНОСТУВАННЯ**
Before starting the first stage of work, the provider must provide the Activity and OCI with a diagnostic strategy, which should include: • Communication protocols with the OCI and the Activity • Format for transferring and receiving documents between supplier, OCI, and the Activity.	Перед початком робіт постачальник повинен надати Проекту та ОКІ стратегію діагностування, яка повинна включати: • Протоколи зв'язку з ОКІ і Проектом. • Формат передачі та отримування документів між постачальником, ОКІ та Проектом. • Визначений Керівник проекту з боку постачальника

• Project manager on the part of the supplier was defined	
REPORT STRUCTURE	**СТРУКТУРА ЗВІТУ**
Each report should consist of five parts: 1. Introduction 2. Goals and tasks performed at the described stage of work 3. Description of mechanisms and approaches used in the report 4. Key Observations - The structure of key observations should follow the structure of the functional areas and domains described in the NIST Cybersecurity Framework 2.0. The report should describe the approach used to determine the current and target maturity level according to the NIST Cybersecurity Framework 2.0. 5. Results of the stage	Кожен звіт повинен складатися з п'яти частин: 1. Вступ 2. Цілі та завдання, що виконуються на описаному етапі роботи 3. Опис механізмів і підходів, використаних у звіті 4. Основні спостереження - Структура ключових спостережень повинна відповідати структурі функціональних областей і доменів, описаних у NIST Cybersecurity Framework 2.0. У звіті повинен бути описаний підхід, який використовувався для визначення поточного та цільового рівня зрілості відповідно до the NIST Cybersecurity Framework 2.0 5. Підсумки етапу
PROCEDURE FOR DIAGNOSTICS AND IMPROVEMENT OF THE CYBERSECURITY MATURITY LEVEL ACCORDING TO THE NIST CYBERSECURITY FRAMEWORK 2.0	**ПОРЯДОК ПРОВЕДЕННЯ РОБІТ З ДІАГНОСТИКИ ТА ПОКРАЩЕННЯ РІВНЯ ЗРІЛОСТІ КІБЕРБЕЗПЕКИ ЗГІДНО NIST CYBERSECURITY FRAMEWORK 2.0**
Stage 1 – Task A. Determining the Recipient's current cybersecurity maturity level Step 1.1 – Determination of the means and methods step 1.1 – Determination of means and methods of communication (letter, e-mail, telephone or other methods) and responsible persons on the part of the recipient and the provider – Project Managers Step 1.2 – Determination of the list of departments, departments, and other structural units that will be involved in the project on the part of the recipient and will be included in the scope of the project - information can be obtained including, but not limited to, from the HR department, specialized information systems and directories of the recipient, and other. Step 1.3 – Determination of strategic goals and objectives of the organization in the field of IT and Cybersecurity. - information can be obtained, including, but not limited to, from the adopted strategic documents of the recipient, which define the goals and objectives of the organization, interviews with the recipient's stakeholders Step 1.4 - Collection of information on the current state of cybersecurity in accordance with the domains and subdomains of the NIST Cybersecurity Framework 2.0 - information can be obtained including, but not limited to, interviews with interested representatives of the recipient, collection of documentary evidence - "artifacts" (acts, procedures, policies, downloads of software settings, contracts, regulatory documents, screenshots) Step 1.5 - Analysis of the information collected in steps 1.2-1.4 for compliance with the requirements of the cyber security domains and subdomains of the NIST Cybersecurity Framework 2.0 - the analysis should	**Етап 1 –Завдання А. Визначення поточного рівня зрілості кібербезпеки Реципієнта** Крок 1.1 – Визначення засобів та методів комунікації (листування, електронна пошта, телефоном чи іншими способами) та відповідальних осіб зі сторони Реципієнта та Підрядника – Менеджерів Проекту Крок 1.2 – Визначення переліку відділів, департаментів та інших структурних одиниць, що будуть залучені до проекту зі сторони Реципієнта та ввійдуть в скоуп проекту – інформація може бути отримана у тому числі, але не обмежуючись - з відділу кадрів, спеціалізованих інформаційних систем та довідників Реципієнта, та інше. Крок 1.3 – Визначення стратегічних цілей та задач організації в області IT та Кібербезпеки. - інформація може бути отримана у тому числі, але не обмежуючись – з прийнятих стратегічних документів Реципієнта, що визначають цілі та задачі організації, інтерв'ю зі стейкхолдерами Реципієнта Крок 1.4 – Збір інформації про поточний стан кібербезпеки відповідно до доменів та субдоменів NIST Cybersecurity Framework 2.0 – інформація може бути отримана у тому числі, але не обмежуючись – з проведення інтерв'ю з зацікавленими представниками Реципієнта, збір документальних доказів – «артефактів» (актів, процедур, політик, вивантажень налаштувань програмного забезпечення, договорів, нормативних документів, знімків екранів) Крок 1.5 – Аналіз зібраної на кроках 1.2-1.4 інформації на відповідність вимогам доменів та субдоменів кібербезпеки NIST Cybersecurity Framework 2.0– аналіз повинен включати в себе опис

include a description of the procedure for checking compliance with the requirements of each subdomain and providing evidence (artifacts) used
Step 1.6 – Based on the information analyzed in step 1.5, determine the current cybersecurity maturity level in accordance with the NIST Cybersecurity Framework 2.0. The maturity level is defined as follows - each subcategory is evaluated on a scale from 0 to 4 points (0 level - 0 points, 1 level - 1 points, 2 level - 2 points, 3 level - 3 points, 4 level - 4 points, the point is assigned in that case - if the sub-domain fully meets the requirements of the maturity level), after which if 0 to 107 points are scored - it is 0 level for the organization as a whole, from 105 to 211 - 1 level, from 212 to 317 - 2 level, from 317 to 423 – 3 level, 424 – 4 level). All points are included when filling (tab Diagnostics (Діагностика)) to the spreadsheet (Forma_Diagnostyky_OKI.xlsm file) provided by the Activity and filled by the provider.
Step 1.7 – Preparation of the report based on the results of stage 1, which includes a completed spreadsheet based on the results of step 1.6
Step 1.8 – Agreeing with the recipient and the Activity of the report based on the results of the stage (within a physical or online meeting)

Stage 2 – Task B. Determination of the Recipient's target cybersecurity maturity level. Development of Recommendations for acquiring the recipient's target cybersecurity maturity level in accordance with the NIST Cybersecurity Framework 2.0. Development of the Roadmap for the implementation of the Recommendations for the acquisition of the target level of the Recipient's cybersecurity maturity in accordance with the NIST Cybersecurity Framework 2.0
Step 2.1 - Conducting interviews with management and key stakeholders to determine key areas for improving cyber security in terms of the organization's goals and objectives - information may be obtained including, but not limited to, the recipient's adopted strategic documents defining the organization's goals and objectives , interviews with the recipient's stakeholders
Step 2.2 – Determination of the available resources of the recipient in the field of cyber security - information can be obtained, including, but not limited to, from existing regulatory and legal documents, a description of the organizational structure, a description of projects, inventory documents, interviews with stakeholders of the recipient
Step 2.3 – Analyze and identify priority cybersecurity categories and subcategories for improvement according to the NIST Cybersecurity Framework 2.0 based on, but not limited to, the results of step 1 and steps 2.1, 2.2.
Step 2.4 - Determination of the target maturity level of cyber security based on the goals, objectives, available and minimum required resources and the results of steps

процедури перевірки на відповідність вимогам кожного субдомена та наведенням використаних доказів (артефактів)
Крок 1.6 – На основі проаналізованої на кроці 1.5 інформації визначення поточного рівня зрілості кібербезпеки у відповідності з NIST Cybersecurity Framework 2.0. Визначення рівня зрілості відбувається наступним чином – кожна субкатегорія оцінюється по шкалі від 0 до 4 балів (0 рівень – 0 бал, 1 рівень – 1 бали, 2 рівень – 2 бали, 3 рівень - 3 бали, 4 рівень – 4 бали, бал присвоюється в тому випадку – якщо субдомен повністю відповідає вимогам рівня зрілості), після чого якщо набрано від 0 до 105 балів – це 0 рівень для організації в цілому, від 106 до 211 – 1 рівень, від 212 до 317 – 2 рівень, від 318 до 423 – 3 рівень, 424 – 4 рівень). Всі бали включаються при заповненні (вкладка Diagnostics (Діагностика) до електронної таблиці (файл Forma_Diagnostyky_OKI.xlsm), що надає Замовник та заповнює Підрядник.
Крок 1.7 – Підготовка Звіту за результатами Етапу 1, що включає в себе заповнену електронну таблицю за результатами Кроку 1.6
Крок 1.8 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 1 (в рамках фізичної чи онлайн зустрічі).

Етап 2 – Завдання В. Визначення цільового рівня зрілості кібербезпеки Реципієнта. Розробка Рекомендацій для набуття цільового рівня зрілості кібербезпеки Реципієнта відповідно NIST Cybersecurity Framework 2.0. Розробка Дорожної Карти впровадження Рекомендацій для набуття цільового рівня зрілості кібербезпеки Реципієнта відповідно до NIST Cybersecurity Framework 2.0

Крок 2.1 – Проведення інтерв'ю з керівництвом та ключовими стейкхолдерами для визначення ключових напрямків покращення кібербезпеки з точки зору цілей та задач організації - інформація може бути отримана у тому числі, але не обмежуючись – з прийнятих стратегічних документів Реципієнта, що визначають цілі та задачі організації, інтерв'ю зі стейкхолдерами Реципієнта
Крок 2.2 – Визначення наявних ресурсів Реципієнта в сфері кібербезпеки - інформація може бути отримана у тому числі, але не обмежуючись – з наявних нормативно-правових документів, опису організаційної структури, опису проектів, інвентаризаційних документів, інтерв'ю зі стейкхолдерами Реципієнта
Крок 2.3 – Аналіз та визначення першочергових, для покращення, категорій та субкатегорій кібербезпеки згідно NIST Cybersecurity Framework 2.0 на основі, але не обмежуючись, результатів Етапу 1 та кроків 2.1, 2.2.

2.1-2.3 and stage 1. The target level of maturity should be at least one higher than the existing one. Step 2.5 – Development of recommendations for increasing the level of maturity of selected cyber security domains and subdomains according to the **NIST Cybersecurity Framework 2.0** based on the results obtained in previous steps Step 2.6 – Development of drafts of necessary documents (including, but not limited to, policies, procedures, instructions) Step 2.7 – Determining the resources required to implement the recommendations developed in step 2.5 and the documents developed in step 2.6 (including, but not limited to, time, personnel, and equipment) Step 2.8 – Development of a 2-month and 3 years Roadmap for the implementation of the developed Recommendations, based on the results of previous steps and, but not limited to, interviews and discussions with stakeholders from the Recipient side Step 2.9 – Developing a report based on the results of Stage 4 and filling in the Recommendation Plan tab (План впровадження рекомендацій) of the spreadsheet (Forma_Daignostyky_OKI.xlsm file) provided by the Activity and completed by the Contractor. The completed spreadsheet tab must be included in the Stage report. Step 2.10 – Preparation of the report based on the results of stage 2 Step 2.11 – Agreeing with the recipient and the Activity of the report based on the results of stage 2 (within a physical or online meeting) **Stage 3 – Tasks C-D. Consultative and methodological support of the Recipient at the stage of implementation of the Road Map Recommendations** Step 3.1 – Provision of monthly advisory support (to the Recipient by the provider at the stage of implementation of the recommendations obtained as a result of stage 2 Step 3.2 – Monitoring by the provider of the progress of the implementation of the recommendations by the Recipient on a monthly basis within the framework of the schedule determined by the Road Map based on the results of Stage 2 Step 3.3 – Submission of a monthly report within 2 months of the implementation of the recommendations provided as a result of Stage 2 and the Road Map, describing the recipient's progress and identified problems and backlogs (if any) Step 3.4 – Agreeing with the Activity of monthly reports based on the results of stage 3 (within a physical or online meeting). **Stage 4 – Task E. Re-diagnostics to confirm the Recipient's achievement of the target cybersecurity maturity level according to the NIST Cybersecurity Framework 2.0**	Крок 2.4 – Визначення цільового рівня зрілості кібербезпеки виходячи з цілей, задач, наявних та мінімальних необхідних ресурсів та результатів Кроків 2.1-2.3 та Етапу 1. Цільовий рівень зрілості має бути не менше ніж на один більший за наявний. Крок 2.5 – Розробка Рекомендацій для підвищення рівня зрілості обраних доменів та субдоменів кібербезпеки **NIST Cybersecurity Framework 2.0**, на основі результатів отриманних на попередніх кроках. Крок 2.6 – Розробка проектів необхідних документів (включаючи, та не обмежуючись - політик, процедур, інструкцій) Крок 2.7 – Визначення ресурсів необхідних для впровадження Рекомендацій розроблених на Кроці 2.5 та документів, розроблених на попередніх кроці 2.6 (включаючи, але не обмежуючись - час, персонал, обладнання) Крок 2.8 – Розробка 2-місячної та 3-річної Дорожньої Карти впровадження розроблених Рекомендацій, на основі результатів попередніх кроків та, але не обмежуючись, інтерв'ю та обговореннями зі стейкхолдерами зі сторони Рецепієнта Крок 2.9 – Розробка звіту за результатами Етапу 4 та заповнення вкладки Recommendation Plan (План впровадження рекомендацій) електронної таблиці (файл Forma_Daignostyky_OKI.xlsm), що надає Замовник та заповнює Підрядник. Заповнена вкладка електронної таблиці повинна бути включена до звіту за Етап. Крок 2.10 – Підготовка звіту за результатами Етапу 2 Крок 2.11 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 2 (в рамках фізичної чи онлайн зустрічі). **Етап 3 – Завдання C-D. Консультативно-методологічна підтримка Реципієнта на етапі впровадження Рекомендацій за Дорожньою Картою** Крок 3.1 – Надання щомісячної консультативної підтримки Реципієнта Підрядником на етапі впровадження Рекомендацій отриманих за результатами Етапу 2 Крок 3.2 – Відслідковування Підрядником прогресу впровадження Рекомендацій Реципієнтом на щомісячній основі в рамках графіку визначеного Дорожньою Картою за результатами Етапу 4 Крок 3.3 – Надання щомісячного звіту протягом 2 місяців впровадження Рекомендацій наданих за результатами Етапу 2 та Дорожної Карти з описом прогресу Реципієнта та виявлених проблем та відставань (за наявності) Крок 3.4 – Погодження з Замовником щомісячних Звітів за результатами виконання Етапу 3 (в рамках фізичної чи онлайн зустрічі). **Етап 4 – Завдання E. Повторна діагностика для підтвердження досягнення Реципієнтом цільового**

Step 4.1 - Gather information on the current state of cybersecurity of NIST Cybersecurity Framework 2.0 domains and subdomains identified in Step 2 as high priority for improvement - information may be obtained including, but not limited to, conducting interviews with interested recipient representatives, collection of documentary evidence - "artifacts" (acts, procedures, policies, downloads of software settings, contracts, regulatory documents, screenshots) Step 4.2 – Analysis of the information collected in step 4.1 for compliance with the requirements of the cyber security domains and subdomains of the NIST Cybersecurity Framework 2.0– the analysis should include a description of the procedure for checking compliance with the requirements of each subdomain and providing evidence (artifacts) used. Step 4.3 - Based on the information analyzed in step 4.2, determine the confirmation of the recipient's achievement of the target level of cybersecurity maturity in accordance with the NIST Cybersecurity Framework 2.0 - the analysis should include a description of the procedure for checking compliance with the requirements of each subdomain and providing evidence (artifacts) used. The maturity level is determined as follows - each subcategory is evaluated on a scale from 0 to 4 points (0 level - 0 points, 1 level - 1 points, 2 level - 2 points, 3 level - 3 points, 4 level - 4 points, the point is assigned in that case - if the sub-domain fully meets the requirements of the maturity level), after which if 0 to 107 points are scored - it is 0 level for the organization as a whole, from 105 to 211 - 1 level, from 212 to 317 - 2 level, from 317 to 423 – 3 level, 424 – 4 level). All points are included when filling (Re-diagnostics tab) into the spreadsheet (Forma_Diagnostyky_OKI.xlsm file) provided by the Activity and filled by the Contractor. Step 4.4 – Preparation of a report based on the results of Stage 4, which includes a completed table based on the results of Step 4.3 Step 4.5 – Agreeing with the recipient and the Activity of the report based on the results of Stage 4 (within a physical or online meeting).	**рівня зрілості кібербезпеки згідно NIST Cybersecurity Framework 2.0** Крок 4.1 – Збір інформації про поточний стан кібербезпеки доменів та субдоменів NIST Cybersecurity Framework 2.0, що були визначені на Етапі 2, як першочергові для Покращення – інформація може бути отримана у тому числі, але не обмежуючись – з проведення інтерв'ю з зацікавленими представниками Реципієнта, збір документальних доказів – «артефактів» (актів, процедур, політик, вивантажень налаштувань програмного забезпечення, договорів, нормативних документів, знімків екранів) Крок 4.2 – Аналіз зібраної на Кроці 4.1 інформації на відповідність вимогам доменів та субдоменів кібербезпеки NIST Cybersecurity Framework 2.0 – аналіз повинен включати в себе опис процедури перевірки на відповідність вимогам кожного субдомена та наведенням використаних доказів (артефактів) Крок 4.3 – На основі проаналізованої на Кроці 4.2 інформації визначення підтвердження досягнення Реципієнтом цільового рівня зрілості кібербезпеки у відповідності з NIST Cybersecurity Framework 2.0 – аналіз повинен включати в себе опис процедури перевірки на відповідність вимогам кожного субдомена та наведенням використаних доказів (артефактів). Визначення рівня зрілості відбувається наступним чином – кожна субкатегорія оцінюється по шкалі від 0 до 4 балів (0 рівень – 0 бал, 1 рівень – 1 бали, 2 рівень – 2 бали, 3 рівень - 3 бали, 4 рівень – 4 бали, бал присвоюється в тому випадку – якщо субдомен повністю відповідає вимогам рівня зрілості), після чого якщо набрано від 0 до 105 балів – це 0 рівень для організації в цілому, від 106 до 211 – 1 рівень, від 212 до 317 – 2 рівень, від 318 до 423 – 3 рівень, 424 – 4 рівень). Всі бали включаються при заповненні (вкладка Re-diagnostics (Повторна діагностика) до електронної таблиці (файл Forma_Diagnostyky_OKI.xlsm), що надає Замовник та заповнює Підрядник. Крок 4.4 – Підготовка звіту за результатами Етапу 4, що включає в себе заповнену таблицю за результатами Кроку 4.3 Крок 4.5 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 4 (в рамках фізичної чи онлайн зустрічі)

Attachment B: Proposal Cover Letter
Додаток В Супровідний лист

We, the undersigned, provide the attached proposal in accordance with RFP No. REQ-KYI-24-0209 dated 17 September 2024. Our attached proposal is for the total price of _____ (figure and in words).

We certify a validity period of 60 (sixty) calendar days for the prices provided in the attached Price Schedule.

We certify our financial responsibility and acceptance of DAI payment terms, which is payment upon delivery and acceptance of the provided services.

Our proposal shall be binding upon us subject to the modifications.

We understand that DAI is not bound to accept any proposals it receives.

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

Telephone:

E-mail:

Company Seal/Stamp:

Ми, що підписалися нижче, надаємо пропозицію із загальною ціною _____ (вкажіть ціну цифрами і прописом), яка додається, відповідно до Запиту на надання пропозиції RFP № REQ-KYI-24-0209 від 17 вересня 2024 року.

Ми засвідчуємо, що ціни зазначені у Прайс-листі, що додається, дійсні протягом періоду 60 (шістдесят) календарних днів.

Ми засвідчуємо нашу фінансову відповідальність і приймаємо умови оплати компанії «DAI», які є оплатою після доставки та прийняття наданих послуг.

Наша пропозиція є обов’язковою для нас з урахуванням змін в результаті будь-яких обговорень.

Ми розуміємо, що компанія «DAI» не зобов’язана приймати будь-які пропозиції, які вона отримує.

Підпис уповноваженої особи:

Ім’я та посада уповноваженої особи:

Назва організації:

Адреса:

Телефон:

E-mail:

Печатка компанії:

Attachment C: Price Schedule / Додаток С: Прайс-лист

The budget below includes examples of the types of costs that may be included in the budget. Actual budget submissions may consist of different costs and should be prepared in line with the offerors' technical proposal. Please include an accompanying budget narrative linking prices with the work required in **Attachment A**. Additional supporting documentation may be requested for any costs included below.

У таблиці нижче наведені вимоги до послуг. Учасники тендеру повинні подати пропозиції, що містять відповідну інформацію на фірмовому бланку або відповідно до офіційного формату пропозиції.

The price could be presented in USD or UAH without VAT/ Усі ціни надані в в доларах США або гривні без ПДВ.

Detailed budget template						**Budget narrative explanation**
Item #	**Item Description/Specifications**	**Unit**	**Quantity**	**Unit Price**	**Total Price**	**Provide brief justification for each line item**
	Опис/Специфікації	Одиниця	Кількість	Ціна за од	Всього	
1	**Program Staffing**					
1,1						
…						
2	**Equipment and material**					
2,1						
…						
3	**Travel, Transportation, Per Diem**					
3,1						
…						
4	**Other Direct Costs/Program Administration and Services**					
4,1						
…						
5	**Benefits/Fee**					
6	**Other Indirect Costs**					
				GRAND TOTAL IN UAH:		

Delivery Period: Click here to enter text.

NOTE: Offerors must submit comprehensive budget narrative/ budget notes that provide information on each line item in the budget and explain why these items are needed to implement the activity, including hourly rates for presented team members and any indirect costs which may occur during the completion of the assessment).

THE PROPOSAL COST/BUDGET MUST BE SUBMITTED IN A PDF AND EXCEL SHEET.

ПРИМІТКА: Учасники повинні подати вичерпний опис бюджету, який містить інформацію про кожну статтю витрат та пояснюють, чому ці статті потрібні для здійснення діяльності, включаючи ціну робочої години спеціалістів та будь-які непрямі витрати, що можуть виникнути в процесі проведення оцінки. Його потрібно надіслати у форматі файлу .pdf та .xls.

Price Schedule / Прайс-лист

№	Milestone No. / Результат	Milestone Description & Required Documentation / Опис та необхідна документація	Payment Amount / Відсоток від суми загальної оплати	Due date / Дата	Total price / Ціна
1	**Milestone #1 / Результат №1**	**Initial Stage:** Signing of the Non-Disclosure Agreement (NDA) between OCI and the selected provider / **Початковий етап**: підписання угоди про нерозголошення (NDA) між OCI та обраним провайдером	35%	20 working days after signing the contract between the selected provider and the Activity / 20 робочих днів після підписання договору між обраним постачальником та Діяльністю	UAH / грн. USD / доллари США
		Deliverable A Report: Assessment of the current OCI cybersecurity maturity level according to the NIST Cybersecurity Framework 2.0 / Звіт за результатами Завдання А: Оцінка поточного рівня зрілості кібербезпеки OCI відповідно до NIST Cybersecurity Framework 2.0		30 working days after signing the NDA between the OCI and the selected provider / 30 робочих днів після підписання NDA між OKI та вибраним постачальником	
2	**Milestone #2 / Результат №2**	Deliverable B Report: Determination of the OCI target maturity level according to NIST Cybersecurity Framework 2.0 Recommendations for transitioning from the current level to the target level. The roadmap for the implementation of the developed recommendations for 2 months and 3 years / Звіт за результатами Завдання В: визначення цільового рівня зрілості OCI відповідно до NIST Cybersecurity Framework 2.0 Рекомендації щодо переходу від поточного рівня до цільового. Дорожня карта реалізації розроблених рекомендацій на 2 місяці та 3 роки	40%	40 working days after the completion of Deliverable A / 40 робочих днів після завершення Завдання А	UAH / грн. USD / доллари США

3	**Milestone #3 / Результат №3**	Deliverable C - D Monthly Report: The progress of implementation of the recommendations by the recipient / Щомісячний звіт за результатами Завдання C - D: хід виконання рекомендацій одержувачем	25%	45 working days after completion of Task B (the report shall capture the work completed under task C and D) / 45 робочих днів після виконання Завдання B (у звіті має бути відображено роботу, виконану за завданнями C та D)	UAH / грн. USD / доллари США
		Deliverable E Report: Reassessment of the current cybersecurity maturity level according to the NIST Cybersecurity Framework 2.0 / Звіт за результатами Завдання E: повторна оцінка поточного рівня зрілості кібербезпеки відповідно до NIST Cybersecurity Framework 2.0		20 working days after the completion of Deliverable C & D / Через 20 робочих днів після завершення Завдань C та D	

Attachment D: Representations and Certifications of Compliance/Додаток D: Заяви та Підтвердженням про Відповідність

1. Federal Excluded Parties List - The Offeror Select is not presently debarred, suspended, or determined ineligible for an award of a contract by any Federal agency.

2. Executive Compensation Certification - FAR 52.204-10 requires DAI, as prime contractor of U.S. federal government contracts, to report compensation levels of the five most highly compensated subcontractor executives to the Federal Funding Accountability and Transparency Act Sub-Award Report System (FSRS).

3. Executive Order on Terrorism Financing - The Contractor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Contractor/Recipient to ensure compliance with these Executive Orders and laws. Recipients may not engage with, or provide resources or support to, individuals and organizations associated with terrorism. No support or resources may be provided to individuals or entities that appear on the Specially Designated Nationals and Blocked persons List maintained by the US Treasury (online at www.SAM.gov) or the United Nations Security Designation List (online at: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml). This provision must be included in all subcontracts/sub awards issued under this Contract.

4. Trafficking of Persons – The Contractor may not traffic in persons (as defined in the Protocol to Prevent, Suppress, and Punish Trafficking of persons, especially Women and Children, supplementing the UN Convention against Transnational Organized Crime), procure commercial sex, and use forced labor during the period of this award.

5. Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions – The Offeror certifies that it currently is and will remain in compliance with FAR 52.203-11, Certification and Disclosure Regarding Payment to Influence Certain Federal Transactions.

6. Organizational Conflict of Interest – The Offeror certifies that will comply FAR Part 9.5, Organizational Conflict of Interest. The Offeror certifies that is not aware of any information bearing on the existence of any potential organizational conflict of interest. The Offeror further certifies that if the Offeror becomes aware of information bearing on whether a potential conflict may exist, that Offeror shall immediately provide DAII with a disclosure statement describing this information.

7. Prohibition of Segregated Facilities - The Offeror certifies that it is compliant with FAR 52.222-21, Prohibition of Segregated Facilities.

1. Федеральний список виключених осіб – Обраний учасник тендера наразі не є відстороненим, тимчасово відстороненим або визнаним таким, що не має права укладати контракт з будь-яким федеральним органом.

2. Підтвердження заробітної плати керівництва – Положення FAR 52.204-10 вимагає від компанії «DAI» як генерального підрядника за контрактами федерального уряду США звітувати про рівні заробітної плати п'яти керівників субпідрядника з найвищим рівнем заробітної плати в Систему звітності за договорами субпідряду відповідно до Закону про підзвітність за федеральним фінансуванням та прозорість (FSRS).

3. Указ Президента США про заборону фінансування тероризму - Виконавцю нагадується, що укази Президента США та законодавство США забороняють здійснювати операції з фізичними особами та організаціями, пов’язаними з тероризмом, а також надавати їм ресурси та підтримку. Юридичну відповідальність за забезпечення дотримання цих указів Президента та законодавства несе Виконавець/Реципієнт. Реципієнту не дозволяється працювати з фізичними особами та організаціями, пов’язаними з тероризмом, а також надавати їм ресурси та підтримку. Жодна допомога або ресурси не можуть надаватись фізичним або юридичним особам, які знаходяться у Списку громадян особливих категорій та заборонених осіб, який веде Казначейство США (див. www.SAM.gov), або у Списку особливих категорій ООН (див. http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml). Це положення обов’язково включається до всіх договорів субпідряду / рішень про надання субпідряду, які виконуються в рамках цього договору.

4. Торгівля людьми – Виконавцю забороняється протягом строку дії цього контракту здійснювати торгівлю людьми (як визначено у Протоколі щодо запобігання, протидії та покарання торгівлі людьми, особливо жінками та дітьми, який доповнює Конвенцію ООН щодо протидії транснаціональної організованої злочинності), оплачувати комерційні сексуальні послуги та використовувати примусову працю.

5. Підтвердження та розкриття інформації щодо платежів з метою впливу на деякі федеральні господарські операції – Учасник тендера підтверджує, що дотримується зараз та дотримуватиметься й надалі вимог FAR 52.203-11 «Підтвердження та розкриття інформації щодо платежів з метою впливу на деякі федеральні господарські операції».

6. Організаційний конфлікт інтересів – Учасник тендеру підтверджує, що йому не відомо про будь-яку інформацію, яка стосується існування будь-якого потенційного конфлікту інтересів організації. Учасник тендеру також підтверджує, що якщо йому стане відомо про інформацію, яка має відношення до можливості існування потенційного конфлікту, Учасник тендеру невідкладно надає компанії «DAI» звіт, де розкривається така інформація.

7. Заборона сегрегації місць спільного користування – Учасник тендера підтверджує, що дотримується FAR 52.222-21 «Заборона сегрегації місць спільного користування».

8. Equal Opportunity – The Offeror certifies that it does not discriminate against any employee or applicant for employment because of age, sex, religion, handicap, race, creed, color or national origin.

9. Labor Laws – The Offeror certifies that it is in compliance with all labor laws.

10. Federal Acquisition Regulation (FAR) – The Offeror certifies that it is familiar with the Federal Acquisition Regulation (FAR) and is in not in violation of any certifications required in the applicable clauses of the FAR, including but not limited to certifications regarding lobbying, kickbacks, equal employment opportunity, affirmation action, and payments to influence Federal transactions.

11. Employee Compliance – The Offeror warrants that it will require all employees, entities and individuals providing services in connection with the Performance of a DAI Purchase Order to comply with the provisions of the resulting Purchase Order and with all Federal, State, and local laws and regulations in connection with the work associated therein.

By submitting a proposal, offerors agree to fully comply with the terms and conditions above and all applicable U.S. federal government clauses included herein and will be asked to sign these Representations and Certifications upon award.

8. Рівні можливості – Учасник тендеру підтверджує, що не здійснює дискримінацію проти будь-якого працівника або заявника за віком, статтю, релігією, інвалідністю, расою, переконаннями, кольором шкіри або національністю.

9. Трудове законодавство – Учасник тендеру підтверджує, що дотримується всіх вимог трудового законодавства.

10. Положення про федеральні закупівлі (FAR) – Учасник тендера підтверджує, що ознайомлений з Положенням про федеральні закупівлі (FAR) і не порушує жодного підтвердження, що вимагається згідно з відповідними нормами FAR, у тому числі, але не обмежуючись підтвердженнями стосовно лобіювання, хабарів, можливості рівного працевлаштування, компенсаційної дискримінації, та платежів з метою впливу на федеральні господарські операції.

11. Дотримання вимог працівниками – Учасник тендеру гарантує, що вимагатиме від усіх працівників, юридичних та фізичних осіб – надавачів послуг у зв'язку з виконанням Договору на закупівлю компанії «DAI» дотримуватись вимог відповідного Договору.

Подаючи пропозицію, учасники тендеру цим погоджуються повністю виконувати умови та положення вищезгаданого та всього відповідного федерального законодавства США, що зазначене у цьому документі, а також при укладенні договору повинні бути готові підписати ці заяви та підтвердження.

Attachment E: Instructions for Obtaining an Unique Entity ID (SAM) for DAI's Vendors, Subcontractors & Grantees / Додаток Е: Інструкції щодо отримання унікального ідентифікатору організації (SAM) – постачальники, субпідрядники та грантоотримувачі компанії «DAI»

Note: The determination of a successful offeror/applicant resulting from this RFP/RFQ/RFA is contingent upon the winner providing an Unique Entity ID (SAM)to DAI. Organizations who fail to provide an Unique Entity ID (SAM) will not receive an award and DAI will select an alternate vendor/subcontractor/grantee.

Note: There is a Mandatory Requirement for your Organization to Provide a Unique Entity ID (SAM) to DAI

I. SUBCONTRACTS/PURCHASE ORDERS: All domestic and foreign organizations which receive first-tier subcontracts/ purchase orders with a value of $30,000 and above are required to obtain an Unique Entity ID (SAM) prior to signing of the agreement. *Your organization is exempt from this requirement if the gross income received from all sources in the previous tax year was under $300,000. Please see the self-certification form attached.*

II. MONETARY GRANTS: All foreign entities receiving first-tier monetary grants (standard, simplified and FAAs) with a value equal to or over $25,000 and performing work outside the U.S. must obtain an Unique Entity ID (SAM) prior to signing of the grant. All U.S. organizations who are recipients of first-tier monetary grants of any value are required to obtain an Unique Entity ID (SAM); the exemption for under $25,000 applies to foreign organizations only.

NO SUBCONTRACTS/POs ($30,000 + above) or MONETARY GRANTS WILL BE SIGNED BY DAI WITHOUT PRIOR RECEIPT OF AN UNIQUE ENTITY ID (SAM).

Background:

Summary of Current U.S. Government Requirements - Unique Entity ID (SAM)

Effective April 4, 2022, entities doing business with the federal government will use the Unique Entity Identifier (SAM) created in SAM.gov. The Unique Entity ID (SAM) is a 12-character alphanumeric value managed, granted, and owned by the government. This allows the government to streamline the entity identification and validation process, making it easier and less burdensome for entities to do business with the federal government.

Entities are assigned an identifier during registration or one can be requested at SAM.gov without needing to register. Ernst and Young provides the validation services for the US Government. The Information required for getting an Unique Entity ID (SAM) without registration is minimal. It only validates your organization's legal business name and address. It is a verification that your organization is what you say it is.

The Unique Entity ID (SAM) does not expire.

Загальна інформація:

Стислий огляд поточних вимог уряду США – унікальний ідентифікатор юридичної особи (SAM)

Починаючи з 4 квітня 2022 року, юридичні особи, які ведуть діяльність із федеральним урядом, використовуватимуть унікальний ідентифікатор юридичної особи (SAM), що створюється на сайті SAM.gov. Унікальний ідентифікатор юридичної особи (SAM) – це 12-значний алфавітно-цифровий код, який контролюється та присвоюється урядом і належить уряду. Він допомагає уряду спростити процес ідентифікації та перевірки юридичних осіб, полегшуючи й роблячи менш обтяжливим для юридичних осіб ведення діяльності з федеральним урядом.

Ідентифікатор надається юридичним особам під час реєстрації, або ж його можна отримати на сайті SAM.gov без реєстрації. Послуги з підтвердження ідентифікатора для уряду США надає компанія *Ernst and Young.* Інформація, необхідна для отримання унікального ідентифікатора юридичної особи (SAM) без реєстрації, – мінімальна. Ідентифікатор підтверджує лише юридичну назву та адресу вашої організації. Це підтвердження того, що ваша організація є тим, за кого себе видає.

Унікальний ідентифікатор юридичної особи (SAM) надається безстроково.

Summary of Previous US Government Requirements – DUNS

The Data Universal Numbering System (DUNS) is a system developed and managed by Dun and Bradstreet that assigns a unique nine-digit identifier to a business entity. It is a common standard world-wide and was previously used by the US Government to assign unique entity identifiers. This system was retired by the US Government on April 4, 2022 and replaced with the Unique Entity Identifier (SAM). After April 4, 2022 the federal government will have no requirements for the DUNS number.

If the entity was registered in SAM.gov (active or inactive registration), a Unique Entity ID (SAM) was assigned and viewable in the entity registration record in SAM.gov prior to the April 4, 2022 transition. The Unique Entity ID (SAM) can be found by signing into SAM.gov and selecting the Entity Management widget in your Workspace or by signing in and searching entity information.

Instructions detailing the process to be followed to obtain a Unique Entity ID (SAM) for your organization begin on the next page.

Стислий огляд колишніх вимог уряду США – DUNS

Універсальна система нумерації даних (DUNS) – це система, розроблена і контрольована компанією *Dun and Bradstreet,* яка присвоює суб'єкту господарювання унікальний дев'ятизначний цифровий ідентифікатор. Така система є світовим стандартом і раніше використовувалась урядом США для присвоєння унікальних ідентифікаторів юридичним особам. 4 квітня 2022 року уряд США припинив використання цієї системи і замінив її на унікальний ідентифікатор юридичної особи (SAM). Після 4 квітня 2022 року федеральний уряд не вимагатиме номер DUNS.

Якщо юридичну особу було зареєстровано на сайті SAM.gov (з активною або неактивною реєстрацією), унікальний ідентифікатор юридичної особи (SAM) був присвоєний і доступний для перегляду в обліковому записі організації на сайті SAM.gov ще до переходу, який відбувся 4 квітня 2022 року. Унікальний ідентифікатор юридичної особи (SAM) можна знайти, увійшовши до системи на сайті SAM.gov і вибравши віджет «Управління організацією / Entity Management» у своєму робочому просторі або увійшовши до системи і виконавши пошук інформації про юридичну особу.

For more information on obtaining the Unique Entity ID/SAM, please visit the link:
https://www.youtube.com/watch?v=4RSHjczdxq8

Offerors shall be informed that they do not need to register for this procurement; they only need to obtain a UE ID. Don't hesitate to contact the CCI Procurement Team for any questions about acquiring a Unique Entity ID.

Attachment F: Information about OCI/ Додаток F: Інформація про ОКІ

The table below provides basic information about the OCI and its scope.

У таблиці нижче наведено базову інформацію про ОКІ та його масштаб.

Name of OCI / Назва ОКІ	**The State of Archival Service of Ukraine/ Державна архівна служба України**
Official Website / Офіційний Веб-сайт	https://archives.gov.ua/
Number of employees / Кількість працівників	68
Number of main divisions (departments) / Кількість основних структурних підрозділів (департаментів)	6
Number of regional offices / Кількість регіональних представництв	1
The number of informational systems, administrated or managed by OKIs / Кількість інформаційних систем, адміністраторами або розпорядниками яких є ОКІ	5

Attachment G: Past Performance/ Додаток G: Досвід роботи

Please indicate orders that best illustrate your work experience relevant to this Request starting from the most recent. The services performed over the past three years will be considered.

Просимо включити замовлення, які найкраще ілюструють ваш досвід роботи, актуальний для цього Запиту, починаючи з останнього замовлення. Беруться до уваги послуги здійснені протягом минулих трьох років.

№	Project Title/ Назва проекту	Description of Activities/ Опис діяльності	Client name/ phone number, e-mail/ Назва клієнта/ номер телефону, e-mail	Price in UAH/ Вартість у грн.	Period of works (Start-End Dates)/ Дати початку і завершення робіт	Completed in time (yes/no)/ Завершено у строк (Так/Ні)	Transfer and acceptance act signed (yes/no)?/ Чи підписано акти приймання-передачі робіт? (Так/Ні)	Type of agreement, subcontract, grant, order (fixed price, with reimbursement of expenses)/ Тип угоди, договору субпідряду, гранту, договору на закупівлю (з фіксованою ціною, з відшкодуванням витрат)
1								
2								
3								
4								
5								

Attachment H: Proposal Checklist/
Додаток Н: Чек-лист пропозиції

Offeror:_____ Have you?

☐ Submitted your proposal to DAI electronic E-mail address UkraineCCI_Proposals@dai.com (as specified in the General Instructions above?

Does your proposal include the following?

☐ Signed Cover Letter *(use template in Attachment B)*

☐ Price Proposal (submitted in PDF and Excel format)

☐ Technical Proposal (including CVs for each team member, Certificates for experts)

☐ Past Performance *(use the template in Attachment G)*.

☐ Documents used to determine Responsibility (As required in section "Responsibility Determination"):

1. Provide copies of the required business licenses to operate in Ukraine (company registration documents, including documents from the tax authority about VAT status).
2. Evidence of a Unique Entity ID (SAM) number for contracts over $30,000
3. The source, origin, and nationality of the services are not from a Prohibited Country.
4. A brief overview of the company, including professional achievements.
5. Confirm that the offeror has enough financial resources to complete the required task.
6. Successful experience with related projects of similar scope and size (see Attachment G)