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

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

REQ-KYI-25-0010

Procurement of technical audit services of the governmental information and communication systems and registries

Закупівля послуг з технічного аудиту державних інформаційно-комунікаційних систем та реєстрів

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

Issue Date: January 23, 2025
Дата: 23 січня 2025 р.

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-25-00010

2. Issue date: January 23, 2025

3. Title

Procurement of technical audit services of the governmental information and communication systems and registries 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

January 30, 2025, 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

February 06, 2025, 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

8. Anticipated Award Type

Firm Fixed Price Purchase Order.

This subcontract type is subject to change during the course of negotiations.

9. Basis for Award

1. Запит № REQ-KYI-25-00010

2. Дата надання запиту: 23 січня 2025 р.

3. Назва

Закупівля послуг з технічного аудиту державних інформаційно-комунікаційних систем та реєстрів 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 **30 січня 2025 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 **06 лютого, 2025 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. Очікуваний вид контракту

Договір на закупівлю із фіксованою ціною.

Цей тип договору субпідряду може бути змінений в процесі проведення переговорів.

9. Підстава для укладення контракту

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 the award, Offerors must meet the requirements identified in Section "Determination of Responsibility."

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 conducts business under the strictest ethical standards to ensure 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 to ethics@dai.com or by visiting www.dai.ethicspoint.com as soon as possible. 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.

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 technical audit of the governmental information and communication systems and registries	Метою цього запиту є отримання пропозицій від постачальників, які зможуть надати послуги для проєкту «USAID Кібербезпека» (далі – Проєкт), який виконується DAI Global LLC, з технічного аудиту державних інформаційно-комунікаційних систем та реєстрів
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 **February 06, 202, 4 p.m.**, Kyiv, Ukraine Time.	• Пропозиції мають бути подані **не пізніше 16:00** за місцевим київським часом в Україні **06 лютого 2025 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

• Offerors shall complete **Attachment C**: Price Schedule. Offerors should indicate the total and all-inclusive service price, 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** per the cooperating country's regulations. 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 **№4464-27 of December 06, 2024**. • Each Offeror and any of its subsidiaries shall submit only one proposal.	Учасника тендеру. Учасник тендеру подає цей лист у форматі .pdf. • 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, **Проєкт 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 **№4464-27 від 06 грудня 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.**	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**

No questions will be answered by phone. Any verbal information received from a DAI, USAID/Cybersecurity employee, or other entity shall not be considered an official response to any question regarding this RFP.	Відповіді на будь-які запитання не будуть надані по телефону. Будь-яка вербальна інформація, отримана від працівника компанії «DAI», або проєкту USAID/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 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 F**.	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 (див. **Додаток F).**

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** (50 points) **Management Approach** (25 points) **Past Performance** (25 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** (50 балів) **Управлінський підхід** (25 балів) **Досвід роботи** (25 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:

Technical Approach / Технічний підхід	Proposals will be evaluated based on the relevance of the proposed solutions to the requirements set forth in the request, including: • a methodological approach to diagnostics to assess the security of information and communication systems, create a list of deficiencies with a description of the risk/consequences and risk level, identify relevant attacker profiles, and create a target system security profile. The methodological approach should be based on the requirements of one or more international standards for conformity assessment • clarity and comprehensibility of the procedure for determining the duration of the work, confirmed by the schedule of the security assessment project. Пропозиції оцінюються виходячи із відповідності запропонованих рішень на основі вимог викладених у запиті, включаючи: • методологічний підхід до проведення діагностики для оцінки захищеності інформаційно-комунікаційних систем, створення списку недоліків з описом ризику/наслідків та рівнем ризику, визначення релевантних профілів зловмисників та створення цільового профілю безпеки системи. Методологічний підхід має ґрунтуватись на вимогах одного чи кількох міжнародних стандартів з оцінки відповідності; • чіткість та зрозумілість процедури визначення тривалості виконання робіт, підтверджена календарним планом проекту оцінки захищеності.	50 points / 50 балів
Client and Management Approach/ Клієнтський та Управлінський підхід	• Availability of certified information and cybersecurity specialists on staff or under employment contracts in sufficient numbers for the list of works. The availability of specialists is confirmed by an extract from the staffing table/copies of orders on appointment to the position or copies of employment contracts • Provided examples of previous experience of proposed staffing team expertise (background, CV) in the field of cybersecurity diagnostics • Copies of certificates confirming the qualifications of employees relevant to the project tasks (primarily internationally recognized certificates). • Наявність сертифікованих спеціалістів з інформаційної та кібербезпеки в штаті або за трудовими договорами у достатній для переліку робіт кількості. Наявність спеціалістів підтверджується витягом з штатного розкладу/копіями наказів про призначення на посаду або копіями трудових договорів; • Підтверджений досвід запропонованого персоналу (кваліфікація, резюме) у сфері проведення діагностик кібербезпеки; • Копії сертифікатів, що підтверджують релевантну задачам проекту кваліфікацію співробітників (передусім - міжнародно визнаними сертифікатами).	25 points / 25 балів
Past Performance / Досвід роботи	• Does the company have experience in carrying out services similar to those outlined in the Scope of Work with USAID-funded projects or technical assistance programs in Ukraine?	25 points / 25 балів

	• Does the company have experience in building information security and cybersecurity systems for government agencies or state-owned enterprises, banking institutions, mobile operators, energy sector companies, and conducting assessments for compliance with international and national cybersecurity standards? • Does the company and its employees have a proven track record of successful implementation of information security projects over the past 3 years in the Ukrainian market or in other countries (preferably the EU, North America, Australia, and the Middle East)? The application must be accompanied by copies of contracts, acts or letters of response with reference to the relevant contracts and acts. • Чи має компанія досвід у наданні послуг подібних до зазначених у технічному завданні проектам, фінансованим USAID або іншим програмам міжнародної технічної допомоги в Україні? • Чи має компанія досвід у сфері побудові систем інформаційної безпеки та кіберзахисту державних органів або державних підприємств, банківських установ, мобільних операторів, компаній енергетичного сектору та проведенні оцінювання на відповідність міжнародним та національним стандартам з кібербезпеки? • Чи має компанія та її співробітники підтверджений досвід успішної реалізації проектів у сфері інформаційної безпеки протягом останніх 3 років на ринку України або інших країн (бажано ЄС, країни північної Америки, Австралії, близького сходу). До заявки мають бути додані копії договорів, актів або листи-відгуки із посиланням на відповідні договори та акти.	
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 **#4464-27 dated December 06, 2024**.	Цінові пропозиції повинні бути надіслані в окремому додатку окремо від технічних пропозицій і мають бути чітко марковані як **«ТОМ ІІ: ЦІНОВА ПРОПОЗИЦІЯ»**. У **Додатку С** надано шаблон Прайс-листа 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 **№4464-27 від 06 грудня 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 F).**	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 F).**
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** Додатково 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 F: 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 F: 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,	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 наступних 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.

Government official, or their representatives, to influence an award or approval decision.
- 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 misstating 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** **Перелік офіційних додатків до цього документу вказаний 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.**

1. Background

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-year period 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.

Component 1: Strengthening the cybersecurity enabling environment

This component will strengthen the cybersecurity resilience of Ukraine's CI sectors by addressing legislative gaps, promoting good governance, enabling collaboration between stakeholders, and supporting cybersecurity institutions. This component will also build the technical capacity of key sectors through increased access to cybersecurity technology and equipment.

Component 2: Developing Ukraine's cybersecurity workforce

This component of the Activity will address workforce gaps through interventions that develop new cybersecurity talent and build the capacity of existing talent. These interventions will address the entire workforce pipeline, the quality of education received by cybersecurity specialists, and industry training programs to rapidly upskill Ukraine's workforce to respond to immediate cybersecurity vulnerabilities.

Component 3: Building a resilient cybersecurity industry

A growing cybersecurity industry in Ukraine will contribute directly to national security and prosperity. This component will seek to build trust and collaboration between the public and private sector to develop innovative solutions for future cybersecurity challenges; spur investment and growth in the broader cybersecurity market in Ukraine through greater access to financing; support smaller cybersecurity companies to rapidly increase the number of local cybersecurity service providers; and offer mechanisms

for Ukrainian firms to connect with industry partners to enable better access to innovations and business opportunities.

2. Context

There is a continued and elevated need in Government of Ukraine to support critical infrastructures and maintain operational functions to keep decision making process and citizens' services ongoing.

Since 2022, state agencies and critical infrastructures have been under constant cyber and physical attacks which altogether requires from them creating robust resilience capabilities, many of which depend on the presence and smart use of digital technologies.

A number of cyberattacks on state information resources in late 2024 and early 2025 point to the need for a comprehensive assessment of the security of important information and communication systems and the development of practical recommendations to improve their protection and resilience.

3. Objectives

The Activity aims to procure services to provide technical audits for the following governmental information and communication systems and registries:

- **Unified state Web portal of electronic services (application and web portal "Diia") / Єдиний державний вебпортал електронних послуг (застосунок та вебпортал "Дія");**
- **System of Electronic Interaction of Electronic Resources (SEIER) / Система електронної взаємодії електронних ресурсів (СЕВ ДЕІР);**
- **Electronic Interaction System of Executive Authorities (EIS EIA) / Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ);**
- **Information and communication system of the central certifying authority / Інформаційно-комунікаційна система центрального засвідчувального органу;**
- **Unified automated information system of customs authorities of the State Customs Service / Автоматизовані інформаційні системи митних органів Державної митної служби;**
- **Central database of the electronic healthcare system of the Ministry of Health / Центральна база даних електронної системи охорони здоров'я Міністерства охорони здоров'я;**
- **State Land Cadastre / Державний земельний кадастр.**

4. Tasks:

DAI/CCI is looking for a qualified **Vendor or consortium of Vendors** to provide list of services based on the Technical Tasks outlined in Annex A for a defined list of information and communication systems and registries.

Annex A. Technical Tasks

Технічне завдання з оцінки захищеності інформаційно-комунікаційних систем	**Technical Task for assessing the security of information and communication systems**
Завдання 1. Встановлення поточного стану технічної та організаційної захищеності систем: • Визначення та опис поточної архітектури систем, їх складових, компонентів та взаємодії між ними. Створення діаграм потоків даних та визначення механізмів їх контролю. Визначення всіх зовнішніх систем, із якими відбувається взаємодія.	**Task 1.** Establishing the current state of technical and organizational security of systems: • Definition and description of the current architecture of the systems, their components, and interactions between them. Creation of data flow diagrams and definition of their control mechanisms. Identification of all external systems with which interaction occurs.

Технічне завдання з оцінки захищеності інформаційно-комунікаційних систем	Technical Task for assessing the security of information and communication systems
• Опис та визначення достатності наявних технічних інструментів та заходів контролю інформаційної та кібербезпеки. • Опис організаційної структури та основних процесів забезпечення кібербезпеки та захисту інформації, оцінка достатності персоналу, верхнерівна оцінка зрілості процесів кібербезпеки. • Перевірка організації управління обліковими записами та повноваженнями: організація, ієрархія, повноваження, ролі, моніторинг та аудит, ідентифікація, автентифікація, деактивація облікових записів, управління сесіями тощо. • Перевірка фактичної моделі розмежування повноважень облікових записів користувачів усіх ролей, перевірка слідування принципу мінімальних привілеїв. • Перевірка організації логічної та фізичної ізоляції мереж та компонентів системи для зменшення потенційної шкоди у випадку компрометації системи (в т.ч. аналіз правил мережевих екранів тощо). • Перевірка фактичного стану процесів аутентифікації: наявність декількох факторів та що це за фактори, обмеження кількості невдалих спроб, реагування на досягнення ліміту невдалих спроб, тощо. • Перевірка ефективності захисту робочих станцій адміністраторів та централізованого управління конфігураціями обладнання та підсистем. • Перевірка фактичного положення управління станами бездіяльності користувача: умови зберігання, блокування та припинення сеансу. • Перевірка фактичної конфігурації віддаленого доступу до системи. • Перевірка поверхні атаки через бездротові мережі, підключені до системи. • Перевірка ефективності управління привілейованим та адміністративним доступом, наявність та налаштування IDM та PAM-інструментів, моніторинг дій адміністраторів та привілейованих користувачів. • Оцінка ефективності процесів навчання персоналу, контролю рівня знань, нагадування про політики безпеки інформації та процедур контролю за змістом публічно доступної інформації. • Визначення достатності процедур тренувального відпрацювання реагування на критичні інциденти, наявності плейбуків тощо • Визначення якості роботи процедур реагування на інциденти: процедури обробки інциденту, правила ескалації, швидкість реакції, документування процесу обробки інциденту, підзвітність, ретроспективний аналіз кожного випадку, ведення історичних даних – реєстру інцидентів, захист даного реєстру. • Визначення ефективності моніторингу подій безпеки, у тому числі з використанням SIEM, якість виявлення загроз через журнали аудиту, якість змісту журналів аудиту, швидкість реагування на	• Description and determination of the adequacy of existing technical tools and information and cybersecurity controls. • Description of the organizational structure and main processes for ensuring cybersecurity and information protection, assessment of staff adequacy, and top-level assessment of the maturity of cybersecurity processes. • Verification of the organization of account and authority management: organization, hierarchy, authority, roles, monitoring and auditing, identification, authentication, account deactivation, session management, etc. • Verification of the actual model of separation of powers of user accounts of all roles, verification of adherence to the principle of least privileges. • Verification of the organization of logical and physical isolation of networks and system components to reduce potential damage in the event of system compromise (including analysis of firewall rules, etc.). • Assessing the actual state of authentication processes: the presence of multiple factors and what they are, limiting the number of failed attempts, responding to reaching the limit of failed attempts, etc. • Verification of the effectiveness of protection of administrator workstations and centralized management of equipment and subsystem configurations. • Verification of the actual status of user inactivity state management: retention, locking, and session termination conditions. • Verification of the actual configuration of remote access to the system. • Assessing the attack surface through wireless networks connected to the system. • Assessing the effectiveness of privileged and administrative access management, the availability and configuration of IDM and PAM tools, and monitoring the actions of administrators and privileged users. • Personnel training processes, knowledge level assessment, and reminders of information security policies and procedures for managing the content of publicly available information. • Determining the adequacy of critical incident response training procedures, availability of playbooks, etc. • Determining the quality of incident response procedures: incident handling procedures, escalation rules, response speed, incident handling process documentation, accountability, retrospective analysis of each case, maintaining historical data – an incident register, and protecting this register. • Determining the effectiveness of security event monitoring, including using SIEM, the quality of threat detection through audit logs, the quality of audit log content, the speed of response to identified threats, protection of audit logs, error handling during auditing, etc. • Definition of processes for managing the configurations of infrastructure elements, its accountability, completeness of the database of configuration elements, and guarantees of the authenticity of exemplary instances.

Технічне завдання з оцінки захищеності інформаційно-комунікаційних систем	Technical Task for assessing the security of information and communication systems
визначені загрози, захист журналів аудиту, обробка помилок при веденні аудиту, тощо. • Визначення процесів управління конфігураціями елементів інфраструктури, її підзвітність, повноти бази конфігураційних елементів, гарантії автентичності зразкових екземплярів. • Перевірка стану програмного забезпечення в мережевому обладнанні: наявність вразливостей на зараз, наявність процедур відстежування появи нових вразливостей, оновлень безпеки та додаткових. Оцінка ефективності процесу patch management. • Оцінка контрольованості організації змін у конфігурацію інфраструктурних елементів: вплив на поточні процеси, на безпеку, на швидкодію, якість методів такого тестування та збереження його артефактів як доказів. • Визначення наявних правил та фактичного управління накопичувачами та носіями інформації: зберігання, організація доступу, знищення, транспортування, використання, маркування, резервне копіювання, тощо. • Базова перевірка організації фізичного доступу до обладнання та робочих місць • Визначення процедур керування ризиком: ідентифікація, аналіз та оцінка ризиків, аналіз достатності описаних ризик-сценаріїв та відповідних заходів контролю, якість виконання цих заходів. • Оцінка захищеності периметру мережі, в т.ч. аналіз периметру на вразливості, перевірка конфігурацій WAF, мережевих екранів, механізмів захисту від DDoS, та інших засобів захисту. • Визначення ризиків безпеки ланцюга постачання програмного забезпечення, в тому числі оцінка заходів перевірки підрядників та постачальників; перевірка безпеки при роботі з ключовими підрядниками з акцентом на вимоги до підрядників під час проведення закупівель, виконання договорів, обмеження доступу до програмного коду та до цільових середовищ систем. • Визначення заходів із запобігання фішингу та їх ефективності. • В разі використання хмарних технологій, або їх елементів, проведення перевірки безпеки архітектури та налаштувань безпеки. • Перевірка процесів безпечної розробки ПЗ, в т.ч. використання інструментів SAST/DAST, методів та інструментів безпечного програмування та деплойменту, в т.ч. з боку підрядників, керування середовищами розробки, тестування та розгортання в продуктовий режим. • Наявність Red Team та перевірка ефективності її роботи. • Оцінка процесів BCP/DRP, достатності механізмів та планів відновлення, оцінка захищеності standby-середовища та резервних копій. • Аналіз ефективності роботи SOC.	• Checking the status of software in network equipment: the presence of current vulnerabilities, procedures for tracking the emergence of new vulnerabilities, security updates, and additional ones. Assessing the effectiveness of the patch management process. • Assessment of the controllability of the organization of changes to the configuration of infrastructure elements: impact on current processes, security, performance, quality of such testing methods, and preservation of its artifacts as evidence. • Determining existing rules and actual management of storage devices and media: storage, access organization, destruction, transportation, use, labeling, backup, etc. • Basic check of the organization of physical access to equipment and workplaces • Definition of risk management procedures: identification, analysis, and assessment of risks, analysis of the adequacy of the described risk scenarios and relevant control measures, and quality of implementation of these measures. • Network perimeter security assessment, including perimeter vulnerability analysis, verification of WAF settings, firewalls, DDoS protection mechanisms, and other protection measures. • Identifying security risks in the software supply chain, including assessing contractor and supplier vetting measures; conducting security audits when working with key contractors; focusing on contractor requirements during procurement and contract execution; and restricting access to software code and target system environments. • Identifying phishing prevention measures and evaluating their effectiveness. • If using the cloud, or its elements, conduct a security audit of the architecture and security settings. • Verification of secure software development processes, including the use of SAST/DAST tools, secure programming and deployment methods and tools, including from contractors, management of development environments, testing, and deployment to production mode. • The presence of a Red Team and verification of its effectiveness. • Assessment of BCP/DRP processes, adequacy of recovery mechanisms and plans, assessment of the security of the standby environment, and backups. • Analysis of SOC performance.

Технічне завдання з оцінки захищеності інформаційно-комунікаційних систем	Technical Task for assessing the security of information and communication systems
Завдання 2. Створення списку недоліків з описом ризику/наслідків та рівнем ризику **Завдання 3**. Визначення релевантних профілів зловмисників, визначення можливого впливу в результаті реалізації зловмисних дій. **Завдання 4.** Рекомендації до усунення виявлених недоліків, перелік заходів, а також функціональні та нефункціональні технічні вимоги до засобів, рекомендованих до впровадження з урахуванням реальних можливостей та специфіки інфраструктури розпорядника та володільця системи. **Завдання 5.** Створення цільового профілю безпеки системи відповідно до міжнародних стандартів та законодавства України	**Task 2.** Creating a list of deficiencies with a description of the risk/consequences and the level of risk **Task 3.** Identifying relevant profiles of attackers, and determining the possible impact as a result of malicious actions. **Task 4.** Recommendations for eliminating the identified shortcomings, a list of measures, and functional and non-functional technical requirements for the tools recommended for implementation, taking into account the system manager's and owner's real capabilities and specifics of the infrastructure. **Task 5.** Creation of a target system security profile in accordance with international standards and Ukrainian legislation

Anticipated post-award Deliverables

Upon award of a subcontract, 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.**

Deliverable	Content	Payment Amount, %	Due to date
Deliverable 1	Report «Current state of technical and organizational security of systems» for each audited organizations based on the materials Task 1 // Звіт «Поточний стан технічної та організаційної захищеності систем», що базується на матеріалах Завдання 1 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу	60%	40 working days from the date of signing the contract
Deliverable 2	Report «List of deficiencies with a description of the risk/consequences and the level of risk» for each audited organizations based on the materials Task 2 // Звіт «Список недоліків з описом ризику/наслідків та рівнем ризику», що базується на матеріалах Завдання 2 Report «Identifying relevant profiles of attackers, and determining the possible impact as a result of malicious actions» for each audited organizations based on the materials Task 3 // Звіт «Релевантні профілі зловмисників, визначення можливого впливу в результаті реалізації зловмисних дій», що базується на матеріалах Завдання 3 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність	20%	50 working days from the date of signing the contract

	Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу		
Deliverable 3	Report «Recommendations for eliminating the identified shortcomings, a list of measures, and functional and non-functional technical requirements for the tools recommended for implementation, taking into account the system manager's and owner's real capabilities and specifics of the infrastructure» for each audited organizations based on the materials Task 4 // Звіт «Рекомендації до усунення виявлених недоліків, перелік заходів, а також функціональні та нефункціональні технічні вимоги до засобів, рекомендованих до впровадження з урахуванням реальних можливостей та специфіки інфраструктури розпорядника та володільця системи», що базується на матеріалах Завдання 4 Report «Target system security profile in accordance with international standards and Ukrainian legislation» for each audited organizations based on the materials Task 5 // Звіт «Цільовий профіль безпеки системи відповідно до міжнародних стандартів та законодавства України», що базується на матеріалах Завдання 5 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу	20%	60 working days from the date of signing the contract

Minimum qualifications, skills, and experience

- The Offeror shall be a duly registered entity in Ukraine and demonstrate this with valid documentation for operation in Ukraine.
- Availability of certified information and cyber security specialists in the staff or under employment contracts in a sufficient number for the list of works
- Confirmed similar successfully completed works both for the market of Ukraine and other countries (preferably the EU, countries of North America, Australia, the Middle East)
- Readiness to sign NDA with recipients (SE Diia, State Custom Services, Ministry of Health, the State Service of Ukraine for Geodesy, Cartography and Cadastre)

Attachment B: Proposal Cover Letter/ Додаток В Супровідний лист

We, the undersigned, provide the attached proposal in accordance with RFP No. REQ-KYI-25-0010 dated 23 January, 2025. 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-25-0010 від 23 січня 2025 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 (on a company's letterhead, signed and stamped) 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 (на офіційному бланку компанії, з підписом та печаткою) та .xls.

Deliverable	Content	Payment Amount, %	Due to date	Total price /Ціна
Deliverable 1	Report «Current state of technical and organizational security of systems» for each audited organizations based on the materials Task 1 // Звіт «Поточний стан технічної та організаційної захищеності систем», що базується на матеріалах Завдання 1 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу	60%	40 working days from the date of signing the contract	UAH/ грн. USD/ долари США
Deliverable 2	Report «List of deficiencies with a description of the risk/consequences and the level of risk» for each audited organizations based on the materials Task 2 // Звіт «Список недоліків з описом ризику/наслідків та рівнем ризику», що базується на матеріалах Завдання 2 Report «Identifying relevant profiles of attackers, and determining the possible impact as a result of malicious actions» for each audited organizations based on the materials Task 3 // Звіт «Релевантні профілі зловмисників, визначення можливого впливу в результаті реалізації зловмисних дій», що базується на матеріалах Завдання 3 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу	20%	50 working days from the date of signing the contract	UAH/ грн. USD/ долари США
Deliverable 3	Report «Recommendations for eliminating the identified shortcomings, a list of measures, and functional and non-functional technical requirements for the tools recommended for implementation, taking into account the system manager's and owner's real capabilities and specifics of the infrastructure» for each audited organizations based on the materials Task 4 // Звіт «Рекомендації до усунення виявлених недоліків, перелік заходів, а також функціональні та нефункціональні технічні вимоги до засобів, рекомендованих до впровадження з урахуванням реальних можливостей та специфіки інфраструктури розпорядника та володільця системи», що базується на матеріалах Завдання 4	20%	60 working days from the date of signing the contract	UAH/ грн. USD/ долари США

	Report «Target system security profile in accordance with international standards and Ukrainian legislation» for each audited organizations based on the materials Task 5 // Звіт «Цільовий профіль безпеки системи відповідно до міжнародних стандартів та законодавства України», що базується на матеріалах Завдання 5 Weekly reports on current and planned activities/ Щотижневі звіти про поточну і заплановану діяльність Recipient's in writing confirmation on the stage completion/Письмове підтвердження Реципієнта про виконання етапу			

Attachment D: Representations and Certifications of Compliance/ Додаток D: Заяви та Підтвердження 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. Рівні можливості – Учасник тендеру підтверджує, що не здійснює дискримінацію проти будь-якого працівника або заявника

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.

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: Past Performance/ Додаток F: Досвід роботи

Please indicate orders that best illustrate your **company** 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 досвід роботи вашої **компанії**, 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 G: Proposal Checklist/ Додаток G: 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 F)*.
- ☐ 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 F).*