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

USAID Cybersecurity for Critical Infrastructure (USAID/Cybersecurity)
USAID Кібербезпека критично важливої інфраструктури (USAID/Кібербезпека)

REQ-KYI-23-0217

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

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

Issue Date: July 25, 2023
Дата: 25 липня 2023

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-23-0217

2. Issue date: July 25, 2023

3. Title

Procurement of services to diagnose the current level of cybersecurity of Public joint-stock company "National Depository of Ukraine" and provide on improving their facilities and strengthening the cyber protection against cyber attacks under USAID Cybersecurity Activity

4. Email address for submission of Proposals

Proposals should be submitted to UkraineCCI_Proposals@dai.com

5. Deadline for Receipt of Questions

August 1, 2023 Kyiv, **18.00** Ukraine Time to the email address UkraineCCI_Procurement@dai.com
All questions will be collected and replies to them will be sent via email to tender participants.

6. Deadline for receipt of Proposals

August 8, 2023 18.00 Kyiv, Ukraine Time to the email address UkraineCCI_Proposals@dai.com

PLEASE NOTE THAT THE EMAIL ADDRESS FOR RECEIPT OF QUESTIONS AND THE EMAIL ADDRESS FOR RECEIPT OF PROPOSALS ARE DIFFERENT

7. Point of contact

UkraineCCI_Procurement@dai.com

8. Anticipated Award Type

Firm Fixed Price Purchase Order

9. Basis for Award

1. Запит № REQ-KYI-23-0217

2. Дата надання запиту: 25 липня 2023

3. Назва

Закупівля послуг діагностування поточного рівня кібербезпеки Публічного акціонерного товариства «Національний Депозитарій України» та надання рекомендації для покращення та посилення рівня захисту від кібер атак в рамках проєкту USAID/Кібербезпека

4. Електронна адреса для подання пропозицій

Пропозиції мають подаватись на адресу: UkraineCCI_Proposals@dai.com

5. Кінцевий термін отримання запитань

18.00 за місцевим київським часом в Україні **1 серпня 2023 року**, на адресу: UkraineCCI_Procurement@dai.com
Всі отримані запитання будуть зібрані, і відповіді на них будуть надіслані учасникам тендеру електронною поштою.

6. Кінцевий термін отримання пропозицій

18.00 за місцевим київським часом в Україні **8 серпня 2023 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

Контракт із фіксованою ціною

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

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 who can provide services to USAID/Cybersecurity Activity (the Activity) DAI Global LLC, to diagnose the current level of cybersecurity of critical infrastructure operators and provide on improving their facilities and strengthening the cyber protection against cyber attacks. Further details on requested services can be found in Attachment C: Price Schedule.	Метою цього запиту є отримання пропозицій від постачальників, які зможуть надати послуги для проєкту «USAID/Кібербезпека» (далі – Проєкт), який виконується DAI Global LLC, з діагностування поточного рівня кібербезпеки об'єктів критичної інфраструктури та надати рекомендації для покращення об'єктам критичної інфраструктури для посилення рівня захисту від кібер атак. Детальна інформація про послуги наведена у Додатку С: Прайс-лист.
Issuing Office	**Офіс, що видає запит на надання пропозицій**
The Issuing Office and Point of Contact noted in the above synopsis are the sole point of contact at DAI for purposes of this RFP. Any prospective Offeror who fails to communicate their interest with this office assumes complete responsibility in the event that they do not receive direct correspondence and relevant information (amendments, answers to questions, etc.) prior to 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 and is not adjusted if the actual costs are higher or lower than the fixed price amount. Offerors are expected to include all costs, direct and indirect, 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 or Ukrainian** 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 або українською мовою** 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 **August 8, 2023, 18:00**, Kyiv, Ukraine Time to the email address.	• Пропозиції мають бути подані **не пізніше 18:00** за місцевим київським часом в Україні **8 серпня 2023 року** на адресу:
• Please note that Offerors shall submit 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 indicates 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 emails.	• У темі повідомлення електронною поштою мають бути зазначені номер Запиту та назву.
• Offerors shall sign, seal and date their proposal cover letter. The Offeror shall submit this letter in .pdf format.	• Усі пропозиції повинні містити супровідний лист, що має дату, підпис та печатку Учасника тендеру. Учасник тендеру подає цей лист у форматі .pdf.

• Offerors shall complete Attachment C: Price Schedule template. Offerors should indicate the total and all-inclusive price for services, roll them up and distribute them across the listed deliverables in the National currency of Ukraine – Hryvnia (UAH) in Attachment C. • **Value Added Tax (VAT) shall not be included in the Price Schedule.** • These services are eligible for VAT exemption on the basis of the USAID Contract №72012120C00002 registered with the Cabinet of Ministers of Ukraine, having the registration card **№4464-11 of June 26, 2023**. • Each Offeror, and any of its subsidiaries, shall submit only one proposal.	• Учасники тендеру заповнюють Додаток С: Прайс-лист. Учасники тендеру повинні вказати загальну та всеосяжну ціну на послуги, загальну ціну та розподілити ціну по вказаних результатах в національній валюті України - гривня в Додатку С. • **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 **№4464-11 від 26 червня 2023 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 email to UkraineCCI_Procurement@dai.com no later than the date specified above. All questions received will be compiled and answered in writing and distributed to all interested Offerors. **Questions should not be submitted to UkraineCCI_Proposals@dai.com** No questions will be answered by phone. Any verbal information received from a DAI or USAID/Cybersecurity employee or other entity shall not be considered an official response to any question regarding this RFP.	Кожен Учасник тендеру є відповідальним за дуже уважне прочитання цього Запиту та повне розуміння його умов. Усе спілкування стосовно цього Запиту має надсилатись електронною поштою на адресу: UkraineCCI_Procurement@dai.com не пізніше дати, зазначеної вище. Всі отримані запитання будуть зібрані, і відповіді на них будуть надіслані електронною поштою усім зацікавленим Учасникам тендеру. **Запитання не мають подаватися за адресою UkraineCCI_Proposals@dai.com** Відповіді на будь-які запитання не будуть надані по телефону. Будь-яка вербальна інформація, отримана від працівника компанії «DAI», або проєкту USAID/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 shall be	Технічні пропозиції повинні бути надіслані в окремому додатку окремо від ціновой пропозиції і мають бути

clearly labeled as "VOLUME I: TECHNICAL PROPOSAL". Technical proposals shall include the following contents: 1. A document in MS Word of approximately maximum 3 pages that responds to the evaluation sub-criteria "Technical Approach". 2. At least 3 references should be provided along with their contact info. Details on nature of work for those clients should be included in Attachment F: Past Performance.	чітко марковані як «ТОМ I: ТЕХНІЧНА ПРОПОЗИЦІЯ». Технічні пропозиції повинні містити такі положення: 1. Документ у MS Word, об'ємом приблизно 3 сторінок, який відповідає підкритеріям оцінки «Технічний підхід». 2. Принаймні 3 рекомендації з контактними даними осіб, які їх надали. Опис характеру роботи для таких клієнтів потрібно надати в додатку F «Досвід роботи».
Services Specified	**Визначення послуг**
For this RFP, DAI is in need of 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, 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. Цінови 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.

Evaluation Criteria/ Критерії оцінки

Technical Approach / Технічний підхід	The proposal is expected to contain the full description of Technical approach and will be evaluated based on how well it addresses the task based on the requirements of the RFP, including: • a detailed methodological approach to conducting diagnostics and evaluating the current level of the cybersecurity level according to the NIST Cybersecurity Framework; • clarity and comprehensibility of the procedure for determining the duration of work; • a methodology for developing recommendations and roadmap for their implementation / consultation support for the object of critical infrastructure, • confirmed experience of work on field of critical infrastructure cybersecurity. Пропозиції оцінюються виходячи із відповідності запропонованих рішень на основі вимог викладених у запиті, включаючи: • детальний методологічний підхід до проведення діагностики, а також оцінювання поточного та цільового рівня кібербезпеки згідно NIST Cybersecurity Framework; • чіткість та зрозумілість процедури визначення тривалості виконання робіт; • методологія розробки рекомендацій, дорожньої карти їх впровадження та консультативної підтримки рецепієнта; • підтверджений досвід роботи в сфері кібербезпеки критичної інфраструктури.	60 points / 60 балів
Client and Management Approach/ Клієнтський та Управлінський підхід	• List of qualified technical specialists assigned to support the Activity and respond to immediate requests. • Confirmed experience of the proposed personnel (qualifications, resume) in the field of conducting cyber security diagnostics of critical infrastructure objects with an indication of the projects in which the personnel participated (a list of relevant projects of each proposed specialist) • At least two qualified technical specialists should hold internationally recognized certificates, such as: CISA, CISM, CISSP, ISO 27001 Lead Assessor, ISO 27001 Lead Implementer, Certified NIST Cybersecurity Framework Lead Implementer • Перелік кваліфікованих технічних спеціалістів наданих на підтримку Проєкту та для відповіді на термінові запити; • Підтверджений досвід запропонованого персоналу (кваліфікація, резюме) у сфері проведення діагностик кібербезпеки об'єктів критичної інфраструктури з вказанням проетків, де песронал приймав участь (перелік відповідних проектів кожного запропонованого спеціаліста) • Кваліфікація принаймні 2 співробітників має бути підтверджена міжнародно визнаними сертифікатами, такими як: CISA, CISM, CISSP, ISO 27001 Lead Assessor, ISO 27001 Lead Implementer, Certified NIST Cybersecurity Framework Lead Implementer.	20 points / 20 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? • Does the company have experience in the field of cybersecurity of critical infrastructure, developing policies and procedures, providing advice, and conducting assessments for compliance with international and national cybersecurity standards, and determining the current and target maturity level of IT processes and cybersecurity processes? • Does the company and its employees have the experience of at least 4 similar projects in the field of information security during the last 3 years? • Does the company have experience in assessing information security at critical infrastructure facilities (such facilities are enterprises that meet the criteria of the Law of Ukraine "On Critical Infrastructure" or are officially included in the list of critical infrastructure facilities)? • 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 кібербезпеки критичної інфраструктури, розробки політик та процедур, наданні консультацій, та проведенні оцінювання на відповідність міжнародним та національним стандартам з кібербезпеки, та визначенні поточного та цільового рівня зрілості ІТ-процесів та процесів кібербезпеки? • Чи має компанія та її співробітники досвід не менше 4 подібних проектів у сфері інформаційної безпеки протягом останніх 3 років? • Чи має компанія досвід оцінки інформаційної безпеки на об’єктах критичної інфраструктури (такими об’єктами є підприємства, що відповідають критеріям Закону України «Про критичну інфраструктуру» або офіційно включені до переліку об’єктів критичної інфраструктури)?	20 points / 20 балів
Total Points / Загальна кількість балів		100 points/ 100 балів

Instructions for the Preparation of the Cost Proposals/ Інструкції щодо підготовки цінових пропозицій

Cost/Price Proposals	**Цінові пропозиції**
Cost/Price proposals shall be sent in a separate attachment from technical proposals and shall be clearly labeled as "VOLUME II: COST/PRICE PROPOSAL". Provided in Attachment C is a template for the Price Schedule, for 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 on the basis of USAID Contract 72012120C00002 registered with the Cabinet of Ministers of Ukraine, having the registration card **#4464-11 dated of June 26, 2023**.	Цінові пропозиції повинні бути надіслані в окремому додатку окремо від технічних пропозицій і мають бути чітко марковані як «ТОМ II: ЦІНОВА ПРОПОЗИЦІЯ». У Додатку С надано шаблон Прайс-листу послуг. Учасники торгів заповнюють шаблон та вказують якомога більше деталей для обгрунтування 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 **№4464-11 від 26 червня 2023 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. 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: 1. Provide copies of the required business licenses to operate in Ukraine (company registration documents, including document 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. Successful experience the firm has with related projects of similar scope and size.	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. 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 задовільного досвіду виконання робіт у минулому.
Anticipated post-award Deliverables	**Очікувані результати після укладення контракту**
Upon award of a subcontract or BPA, the deliverables and deadlines detailed in the below table will be submitted to DAI. The Offeror should detail proposed costs per deliverable in the Price Schedule. All of the deliverables must be submitted to and approved by DAI before payment will be processed. See Attachment C: Price Schedule for more information on the anticipated post-award deliverables.	Після укладення субконтракту або Рамкового договору про закупівлю, 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. Дивись 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 performed in a satisfactory manner, and that all equipment or supplies are of acceptable quality and standards. The Subcontractor shall be responsible for any countermeasures or corrective action, within the scope of this RFP, which may be required by the DAI Chief of Party 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. Субпідрядник несе відповідальність за будь-які контрзаходи або коригувальні дії в межах цього Запиту на надання пропозицій, які можуть вимагатись Керівником проєкту компанії «DAI» за результатами такої перевірки.
Compliance with Terms and Conditions In addition to comply with the foresaid requirements, the Offerors are required to fully meet or exceed the significant not cost- related specifications: 1. Offeror must be registered in Ukraine as demonstrated by valid documents for operation in Ukraine (company registration documents, including document from the tax authority about VAT status).	**Відповідність вимогам** На додаток до відповідності вищезазначеним вимогам, Учасники повинні повністю відповідати або перевищувати неціновим вимогам специфікації: 1. Учасник повинен бути зареєстрований в Україні, що підтверджується чинними документами для діяльності в Україні (реєстраційні документи

2. Consent to receive payment for services solely by bank transfer. 3. Offeror must have a minimum of 3 years of relevant experience in provision of similar services (please fill Attachment G: Past Performance). Offeror must have adequate financial resources to perform the work within the required delivery schedule, as evidenced by acceptance of DAI payment terms upon delivery and acceptance by DAI as stated in cover letter.	компанії, у тому числі документ від податкового органу про статус ПДВ). 2. Згода на отримання оплати послуг виключно банківським переказом. 3. Учасник повинен мати не менше 3 років відповідного досвіду надання подібних послуг (будь ласка, заповніть Додаток G: Попередній досвід). Учасник повинен мати достатні фінансові ресурси для виконання робіт у 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. Geographic Code 937: 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	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. Географічний код 937: 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

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.	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 which receive 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 prior to signing of the agreement. Organizations are exempt from this requirement if the gross income received from all sources in the previous tax year was under $300,000. DAI requires that Offerors sign the self-certification statement if the Offeror claims exemption for this reason. For those required to obtain a SAM ID number, you may see Instructions for Obtaining a SAM ID number (see Attachment E). For those not required to obtain a SAM ID number, you may see Attachment: Self-Certification for Exemption from SAM ID Requirement (see Attachment F).	Всі американські та іноземні організації, які отримують субконтракти/ договори на закупівлю на суму в еквіваленті 30 000 доларів США і вище, **повинні** отримати унікальний ідентифікатор організації (SAM) до підписання угоди. Організації звільняються від цієї вимоги, якщо валовий дохід, отриманий з усіх джерел за попередній податковий рік, був нижче 300 000 доларів США. Компанія «DAI» вимагає, щоб Учасники тендеру підписали заяву про самовизначення, якщо вони вимагають звільненя з цієї причини. Для тих, кому потрібно отримати унікальний ідентифікатор організації (SAM), зверніться до Інструкції для отримання унікального ідентифікатору організації (SAM) (Дивись Додаток Е). Для тих, хто не зобов'язаний отримувати унікальний ідентифікатор організації (SAM), зверніться до Форми самовизначення на звільнення від вимоги отримання унікального ідентифікатору організації (SAM) (Дивись Додаток F).
Anti-Corruption and Anti-Bribery Policy and Reporting Responsibilities	**Політика щодо боротьби з корупцією та боротьбою з хабарництвом та Відповідальної Звітності**
• DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful performance or delivery of quality goods and equipment. **DAI does not tolerate the following acts of corruption:** • Any requests for a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special consideration by a DAI employee, Government official, or their representatives, to influence an award or approval decision. • Any offer of a bribe, kickback, facilitation payment or gratuity in the form of payment, gift or special	DAI веде свою діяльність за найсуворішими етичними стандартами, щоб забезпечити чесність конкуренції, прийнятні ціни та успішне надання послуг або доставку якісних товарів та обладнання. **DAI не терпить таких корупційних дій:** • Будь -які запити на отримання хабара, віддачі, сприяння чи виплати у вигляді виплати, подарунка або спеціальної компенсації співробітнику DAI, урядовцю чи їх представникам впливають на рішення про нагородження або схвалення • Будь -яка пропозиція хабара, відкату, сприяння чи виплати у вигляді платежу, подарунка або спеціальної винагороди від оферента чи

consideration by an offeror or subcontractor to influence an award or approval decision. • Any fraud, such as mis-stating or withholding information to benefit the offeror or subcontractor. • Any collusion or conflicts of interest in which a DAI employee, consultant, or representative has a business or personal relationship with a principal or owner of the offeror or subcontractor that may appear to unfairly favor the offeror or subcontractor. Subcontractors must also avoid collusion or conflicts of interest in their procurements from vendors. Any such relationship must be disclosed immediately to DAI management for review and appropriate action, including possible exclusion from award. • These acts of corruption are not tolerated and may result in serious consequences, including termination of the award and possible suspension and debarment by the U.S. Government, excluding the offeror or subcontractor from participating in future U.S. Government business. • Any attempted or actual corruption should be reported immediately by either the offeror, subcontractor or DAI staff to: • Toll-free Ethics and Compliance Anonymous Hotline at (U.S.) +1-503-597-4328 • Hotline website – www.DAI.ethicspoint.com, or Email 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.	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** **Дивись перелік офіційних додатків до цього документу нижче.**

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

The below contains the technical requirements of the services. Offerors are requested to provide proposals containing the information below on official letterhead or official proposal format.

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

Background	**Передумови**
The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the 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 Critical Infrastructure (CI), and to transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. Over a five-year period, the Activity will increase resilience and build capacity to prevent, detect, and respond to cyberattacks against CI in Ukraine. To achieve this goal, the Activity is implementing the following components: **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	Проєкт USAID «Кібербезпека критично важливої інфраструктури України» (далі – Проєкт) фінансується USAID та реалізується DAI. Кінцева мета Проєкту – розвиток національної системи кібербезпеки та зменшення кількості вразливостей критично важливої інфраструктури. Протягом п'яти років Проєкт зміцнюватиме стійкість і розвиватиме спроможність запобігати, виявляти й боротися з кібератаками, націленими на критичну інфраструктуру (далі – КІ) України. Для цього Проєкт реалізовує такі складові: **Компонент 1**: Посилення сприятливого середовища для кібербезпеки Цей компонент посилить стійкість секторів КІ України до кібербезпеки шляхом усунення прогалин у законодавстві, сприяння належному управлінню, сприяння співпраці між зацікавленими сторонами та підтримки установ кібербезпеки. Цей компонент також розширить технічну спроможність ключових секторів за рахунок розширення доступу до технологій та обладнання кібербезпеки. **Компонент 2**: Розвиток кадрів з кібербезпеки в Україні Цей компонент діяльності спрямований на усунення недоліків робочої сили за допомогою втручань, спрямованих на розвиток нових спеціалістів із кібербезпеки та нарощування потенціалу наявних спеціалістів. Ці заходи стосуватимуться всього кадрового потенціалу, якості освіти, отриманої фахівцями з кібербезпеки, і галузевих навчальних програм для швидкого підвищення навичок української

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.	робочої сили для реагування на миттєві вразливості кібербезпеки. **Компонент 3:** Створення стійкої галузі кібербезпеки Зростання галузі кібербезпеки в Україні безпосередньо сприятиме національній безпеці та процвітанню. Цей компонент буде спрямований на зміцнення довіри та співпраці між державним і приватним секторами для розробки інноваційних рішень для майбутніх проблем кібербезпеки; стимулювати інвестиції та зростання ширшого ринку кібербезпеки в Україні за рахунок розширення доступу до фінансування; підтримувати невеликі компанії з кібербезпеки для швидкого збільшення кількості місцевих постачальників послуг з кібербезпеки; а також запропонувати українським компаніям механізми зв'язку з галузевими партнерами, щоб забезпечити кращий доступ до інновацій та можливостей для бізнесу.
Context	**Контекст**
The Activity provides assistance to critical infrastructure objects in the energy and other sectors (hereinafter - OCI - within the meaning of the Law of Ukraine "On Critical Infrastructure" or officially included in the list of critical infrastructure objects) in strengthening their resistance to cybersecurity incidents. At the request of OCI, the Activity plans to conduct diagnostics of their cybersecurity systems. The result of the diagnosis will be an assessment of the current level of maturity of the OCI. The diagnosis is carried out in accordance with the NIST Cybersecurity Framework, and based on the results, recommendations will be developed to improve the cyber resilience of the organization in accordance with the NIST Cybersecurity Framework. The results of the diagnostic will also establish a basis for measuring the progress of strengthening the cyber resilience of the OCI after the implementation of the recommendations provided after the diagnosis	Проект надає допомогу об'єктам критичної інфраструктури в енергетичному та інших секторах (далі – ОКІ – у розумінні Закону України «Про критичну інфраструктуру» або офіційно включені до переліку об'єктів критичної інфраструктури) у посиленні їх стійкості до інцидентів кібербезпеки. На запит ОКІ Проект планує проведення діагностування кібербезпеки їх систем. Результатом діагностування буде оцінка поточного рівня зрілості ОКІ. Діагностування здійснюється у відповідності до NIST Cybersecurity Framework, а за результатами будуть розроблені рекомендації щодо підвищення кіберстійкості організації відповідно до NIST Cybersecurity Framework. Результати діагностування також встановлять основу для вимірювання прогресу посилення кіберстійкості ОКІ після впровадження рекомендацій, наданих після діагностування.
Objectives	**Цілі**
The overall goal of the task is to conduct a diagnosis of the cybersecurity system of CIO to assess the level of cyber maturity in accordance with the requirements of the NIST Cybersecurity Framework and provide recommendations for improving the state of cyber readiness	Загальна мета завдання полягає в тому, щоб провести діагностування системи кібербезпеки ОКІ для оцінки рівня кіберзрілості відповідно до вимог NIST Cybersecurity Framework та надати рекомендації щодо покращення стану кіберготовності
Tasks	**Задачі**

Carrying out diagnostic of Public joint-stock company "National Depository of Ukraine" (see Appendix H) (next – CIO or Recepient) cybersecurity systems, which will include the following steps performed in accordance with the NIST Cybersecurity Framework: a. Assessment of the current level of maturity of the cyber security of CIO according to the NIST Cybersecurity Framework and penetration testing according to the "Gray box" model for 25 IP addresses in 120 servers and 30 systems and using social engineering methods. b. Determining the target level of CIO maturity according to the NIST Cybersecurity Framework c. Development of recommendations for the transition from the current level to the target level. Recommendations should contain a list of necessary policies and processes of information (cyber) security, calculation of necessary resources, definition of personnel competencies, organizational structure. Also, based on the received recommendations, drafts of 10 information security policies should be developed, recommendations for existing procedures and policies developed, recommendations for NGFW (FortiGate), WAF (FortiWeb), Microsoft Active Directory equipment settings developed; and a high-level design (HLD) of the cyber security architecture (including an operational model) and a technical specification with an approximate estimate of the cost of implementing the developed architecture should also be developed. d. Development of a road map for the implementation of the developed recommendations for 4 months. The road map should contain a list of measures that the CIO should take to achieve the target level of maturity with a detailed description of each of them and the necessary resources for their implementation.	Проведення діагностування системи кібербезпеки Публічного акціонерного товариства «Національний Депозитарій України» (див. Додаток Ґ) (далі – ОКІ або Реципієнт), що буде включати в себе наступні крокі виконані відповідно до NIST Cybersecurity Framework: a. Оцінювання поточного рівня зрілості кібербезпеки ОКІ відповідно до NIST Cybersecurity Framework та тестування на проникнення за моделлю “Gray box” для 25 IP-адрес в 120 серверів та 30 систем та з використанням методів соціальної інженерії. b. Визначення цільового рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework c. Розробка рекомендацій щодо переходу від поточного рівня до цільового рівня. Рекомендації повинні містити перелік необхідних політик та процесів інформаційної (кібер) безпеки, підрахунок необхідних ресурсів, визначення компетенцій персоналу, організаційну структуру. Також на основі отриманих рекомендацій повинні бути розроблені проекти 10 політик інформаційної безпеки, розроблені рекомендації до наявних процедур та політик, розроблені рекомендації для налаштувань обладнання NGFW (FortiGate), WAF (FortiWeb), Microsoft Active Directory; а також має бути розроблено високорівневий дизайн (HLD) архітектури кібербезпеки (включно із операційною моделлю) та технічна специфікація з орієнтовною оцінкою вартості впровадження розробленої архітектури. d. Розробка дорожньої карти реалізації розроблених рекомендацій на 4 місяці. Дорожня карта повинна містити список заходів, що має вжити ОКІ для досягнення цільового рівня зрілості з детальним

e. Provision of 6 days of advisory support to the CIO in the process of implementation of the provided recommendations by the CIO. f. Development of a monthly report on the progress of implementation of the recommendations provided by the CIO. g. Evaluation of the maturity level of CIO 's cyber security systems in accordance with the NIST Cybersecurity Framework after 4 months from the date of receipt of the CIO 's recommendations.	описом кожного з них та визначеними для їх вжиття необхідних ресурсів. e. Надання 6 днів консультативної підтримки ОКІ в процесі впровадження ОКІ наданих рекомендацій. f. Розробка щомісячного звіту про хід виконання рекомендацій наданих ОКІ. g. Оцінювання рівня зрілості систем кібербезпеки ОКІ відповідно до NIST Cybersecurity Framework через 4 місяці з дати отримання ОКІ рекомендацій.

Deliverables schedule		**Графік надання результатів**	
Task A Report: Assessment of the current OCI cybersecurity maturity level according to the NIST Cybersecurity Framework	30 working days from the beginning of the assessment	Звіт про завдання А: Оцінка рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework	30 робочих днів з моменту початку оцінювання
Task B Report: Determination of the OCI target maturity level according to NIST Cybersecurity Framework.	10 working days after the completion of Task A	Звіт про завдання В: Визначення цільового рівня зрілості ОКІ відповідно до NIST Cybersecurity Framework.	10 робочих днів після виконання завдання А
Task C Report: Recommendations for the transition from the current level to the target level.	20 working days after the completion of Task B	Звіт про завдання С: Рекомендації щодо переходу від поточного рівня до цільового рівня зрілості.	Через 20 робочих днів після виконання завдання В
Task D Report: The Road map for the implementation of the developed recommendations for a period of 4 months	10 working days after the completion of Task C	Звіт про завдання D: Дорожня карта впровадження розроблених рекомендацій на 4 місяці	10 робочих днів після виконання завдання С
Task E - F Monthly Report: The progress of implementation of the recommendations by the recipient	Monthly report during 4 months of realization tasks E and F.	Щомісячний звіт по Завданню Е та F: Надання консультативної підтримки підрядником для ОКІ	Щомісячний звіт протягом 4х місяців виконання завдань Е та F.
Task G Report: Reassessment of the current cybersecurity maturity level according to the NIST Cybersecurity Framework.	20 working days after the completion of Task F	Звіт про завдання G: повторна оцінка рівня зрілості кібербезпеки відповідно до NIST Cybersecurity Framework.	20 робочих днів після виконання Завдання F
Minimum qualifications, skills and experience		**Мінімальна кваліфікація, навички та досвід**	
1. The supplier must be registered and provide auditing, assessment or consulting services		1. Постачальник має бути зареєстровий та надавати послуги з аудиту, оцінювання	

in the field of cybersecurity in Ukraine within 1 year; 2. Employees of the supplier must have experience in conducting at least 2 similar information security diagnostic projects during the last 5 years; 3. The qualification of at least 2 employees of supplier must be confirmed by internationally recognized certificates, for example: CISA, CISM, CISSP, ISO 27001 Lead Assessor, ISO 27001 Lead Implementer, Certified NIST Cybersecurity Framework Lead Implementer or any other international certifications in informational security; 4. Confirmed experience of the proposed personnel (qualifications, resume) in the field of conducting cyber security diagnostics with an indication of the projects in which the personnel participated (a list of relevant projects of each proposed specialist)	чи консультування в сфері кібербезпеки в Україні протягом 1 року; 2. Співробітники постачальника повинні мати досвід у проведенні не менше 2 подібних проектів діагностування інформаційної безпеки протягом останніх 5 років; 3. Кваліфікація принаймні 2 співробітників постачальника має бути підтверджена міжнародно визнаними сертифікатами, наприклад: CISA, CISM, CISSP, ISO 27001 Lead Assessor, ISO 27001 Lead Implementer, Certified NIST Cybersecurity Framework Lead Implementer або інші міжнародні сертифікації в області інформаційної безпеки; 4. Підтверджений досвід запропонованого персоналу (кваліфікація, резюме) у сфері проведення діагностик кібербезпеки з вказанням проектів, де персонал приймав участь (перелік відповідних проектів кожного запропонованого спеціаліста)
DIAGNOSTIC STRATEGY	**СТРАТЕГІЯ ДІАГНОСТУВАННЯ**
Before starting the first stage of work, the supplier must provide to the Activity and OCI an diagnostic strategy, which should include: • Communication protocols with the OCI and the Activity • Format for transferring and receiving documents between supplier, OCI and the Activity. • Project manager on the part of the supplier was defined	Перед початком робіт постачальник повинен надати Проекту та ОКІ стратегію діагностування, яка повинна включати: • Протоколи зв'язку з ОКІ і Проектом. • Формат передачі та отримування документів між постачальником, ОКІ та Проектом. • Визначений Керівник проекту з боку постачальника
REPORT STRUCTURE	**СТРУКТУРА ЗВІТУ**
Each report should consist of five parts: 1. Introduction 2. Goals and tasks performed at the described stage of work 3. Description of mechanisms and approaches used in the report 4. Key Observations - The structure of key observations should follow the structure of the functional areas and domains described in the NIST Cybersecurity Framework. The report should describe the approach used to determine the current and target maturity	Кожен звіт повинен складатися з п'яти частин: 1. Вступ 2. Цілі та завдання, що виконуються на описаному етапі роботи 3. Опис механізмів і підходів, використаних у звіті 4. Основні спостереження - Структура ключових спостережень повинна відповідати структурі функціональних областей і доменів, описаних у NIST Cybersecurity Framework. У звіті повинен бути описаний підхід, який використовувався для визначення

level according to the NIST Cybersecurity Framework. 5. Results of the stage	поточного та цільового рівня зрілості відповідно до the NIST Cybersecurity Framework. 5. Підсумки етапу
PROCEDURE FOR DIAGNOSTICS AND IMPROVEMENT OF THE CYBERSECURITY MATURITY LEVEL ACCORDING TO THE NIST CYBERSECURITY FRAMEWORK	**ПОРЯДОК ПРОВЕДЕННЯ РОБІТ З ДІАГНОСТИКИ ТА ПОКРАЩЕННЯ РІВНЯ ЗРІЛОСТІ КІБЕРБЕЗПЕКИ ЗГІДНО NIST CYBERSECURITY FRAMEWORK**
Stage 1 – Determining the Recipient's current cybersecurity maturity level Step 1.1 – Determination of the means and methods Step 1.1 – Determination of means and methods of communication (letter, e-mail, telephone or other methods) and responsible persons on the part of the Recipient and the Contractor – Project Managers Step 1.2 – Determination of the list of departments, departments and other structural units that will be involved in the project on the part of the Recipient and will be included in the scope of the project - information can be obtained including, but not limited to, from the HR department, specialized information systems and directories of the Recipient, and other. Step 1.3 – Determination of strategic goals and objectives of the organization in the field of IT and Cybersecurity. - information can be obtained, including, but not limited to, from the adopted strategic documents of the Recipient, which define the goals and objectives of the organization, interviews with the Recipient's stakeholders Step 1.4 - Collection of information on the current state of cybersecurity in accordance with the domains and subdomains of the NIST Cybersecurity Framework - information can be obtained including, but not limited to, interviews with interested representatives of the Recipient, collection of documentary evidence - "artifacts" (acts, procedures, policies, downloads of software settings, contracts, regulatory documents, screenshots) Step 1.5 - Analysis of the information collected in steps 1.2-1.4 for compliance with the requirements of the cyber security domains and subdomains of the NIST Cybersecurity Framework - the analysis should include a description of the procedure for checking compliance with the requirements of each subdomain and providing evidence (artifacts) used Step 1.6 – Based on the information analyzed in step 1.5, determine the current cybersecurity maturity level in accordance with the NIST	**Етап 1 – Визначення поточного рівня зрілості кібербезпеки Реципієнта** Крок 1.1 – Визначення засобів та методів комунікації (листування, електронна пошта, телефоном чи іншими способами) та відповідальних осіб зі сторони Реципієнта та Підрядника – Менеджерів Проекту Крок 1.2 – Визначення переліку відділів, департаментів та інших структурних одиниць, що будуть залучені до проекту зі сторони Реципієнта та ввійдуть в скоуп проекту – інформація може бути отримана у тому числі, але не обмежуючись - з відділу кадрів, спеціалізованих інформаційних систем та довідників Реципієнта, та інше. Крок 1.3 – Визначення стратегічних цілей та задач організації в області IT та Кібербезпеки. - інформація може бути отримана у тому числі, але не обмежуючись – з прийнятих стратегічних документів Реципієнта, що визначають цілі та задачі організації, інтерв'ю зі стейкхолдерами Реципієнта Крок 1.4 – Збір інформації про поточний стан кібербезпеки відповідно до доменів та субдоменів NIST Cybersecurity Framework– інформація може бути отримана у тому числі, але не обмежуючись – з проведення інтерв'ю з зацікавленими представниками Реципієнта, збір документальних доказів – «артефактів» (актів, процедур, політик, вивантажень налаштувань програмного забезпечення, договорів, нормативних документів, знімків екранів) Крок 1.5 – Аналіз зібраної на кроках 1.2-1.4 інформації на відповідність вимогам доменів та субдоменів кібербезпеки NIST Cybersecurity Framework– аналіз повинен включати в себе опис процедури перевірки на відповідність вимогам кожного субдомена та наведенням використаних доказів (артефактів) Крок 1.6 – На основі проаналізованої на кроці 1.5 інформації визначення поточного рівня зрілості кібербезпеки у відповідності з NIST

Cybersecurity Framework. The maturity level is determined as follows - each subcategory is evaluated on a scale from 1 to 5 points (0 level - 0 points, 1 level - 1 points, 2 level - 2 points, 3 level - 3 points, 4 level - 4 points, the point is assigned in that case - if the sub-domain fully meets the requirements of the maturity level), after which if 0 to 107 points are scored - it is 0 level for the organization as a whole, from 108 to 215 - 1 level, from 216 to 323 - 2 level, from 324 to 431 – 3 level, 432 – 4 level). All points are included when filling (tab Diagnostics (Діагностика)) to the spreadsheet (Forma_Diagnostyky_OKI.xlsm file) provided by the Activity and filled by the Contractor. Step 1.7 – Preparation of the Report based on the results of Stage 1, which includes a completed spreadsheet based on the results of Step 1.6 Step 1.8 – Agreement with the Recipient and the Activity of the Report based on the results of the Stage **Stage 2 – Determination of the Recipient's target cybersecurity maturity level** Step 2.1 - Conducting interviews with management and key stakeholders to determine key areas for improving cyber security in terms of the organization's goals and objectives - information may be obtained including, but not limited to, the Recipient's adopted strategic documents defining the organization's goals and objectives , interviews with the Recipient's stakeholders Step 2.2 – Determination of the available resources of the Recipient in the field of cyber security - information can be obtained, including, but not limited to, from existing regulatory and legal documents, a description of the organizational structure, a description of projects, inventory documents, interviews with stakeholders of the Recipient Step 2.3 – Analyze and identify priority cybersecurity categories and subcategories for improvement according to the NIST Cybersecurity Framework based on, but not limited to, the results of Step 1 and Steps 2.1, 2.2. Step 2.4 - Determination of the target maturity level of cyber security based on the goals, objectives, available and minimum required resources and the results of Steps 2.1-2.3 and Stage 1. The target maturity level should be no more than one greater than the existing one.	Cybersecurity Framework. Визначення рівня зрілості відбувається наступним чином – кожна субкатегорія оцінюється по шкалі від 1 до 5 балів (0 рівень – 0 бал, 1 рівень – 1 бали, 2 рівень – 2 бали, 3 рівень - 3 бали, 4 рівень – 4 бали, бал присвоюється в тому випадку – якщо субдомен повністю відповідає вимогам рівня зрілості), після чого якщо набрано від 0 до 107 балів – це 0 рівень для організації в цілому, від 108 до 215 – 1 рівень, від 216 до 323 – 2 рівень, від 324 до 431 – 3 рівень, 432 – 4 рівень). Всі бали включаються при заповненні (вкладка Diagnostics (Діагностика) до електронної таблиці (файл Forma_Diagnostyky_OKI.xlsm), що надає Замовник та заповнює Підрядник. Крок 1.7 – Підготовка Звіту за результатами Етапу 1, що включає в себе заповнену електронну таблицю за результатами Кроку 1.6 Крок 1.8 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 1. **Етап 2 – Визначення цільового рівня зрілості кібербезпеки Реципієнта** Крок 2.1 – Проведення інтерв'ю з керівництвом та ключовими стейкхолдерами для визначення ключових напрямків покращення кібербезпеки з точки зору цілей та задач організації - інформація може бути отримана у тому числі, але не обмежуючись – з прийнятих стратегічних документів Реципієнта, що визначають цілі та задачі організації, інтерв'ю зі стейкхолдерами Реципієнта Крок 2.2 – Визначення наявних ресурсів Реципієнта в сфері кібербезпеки - інформація може бути отримана у тому числі, але не обмежуючись – з наявних нормативно-правових документів, опису організаційної структури, опису проектів, інвентаризаційних документів, інтерв'ю зі стейкхолдерами Реципієнта Крок 2.3 – Аналіз та визначення першочергових, для покращення, категорій та субкатегорій кібербезпеки згідно NIST Cybersecurity Framework на основі, але не обмежуючись, результатів Етапу 1 та кроків 2.1, 2.2. Крок 2.4 – Визначення цільового рівня зрілості кібербезпеки виходячи з цілей, задач, наявних та мінімальних необхідних ресурсів та результатів Кроків 2.1-2.3 та Етапу 1. Цільовий рівень зрілості має бути не більше ніж на один більший за наявний.

Step 2.5 – Preparation of the report based on the results of Stage 2 Step 2.6 – Agreement with the Recipient and the Activity of the Report based on the results of Stage 2	Крок 2.5 – Підготовка звіту за результатами Етапу 2 Крок 2.6 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 2.
Stage 3 – Stage 3 – Development of Recommendations for acquiring the Recipient's target cybersecurity maturity level in accordance with the NIST Cybersecurity Framework Step 3.1 – Development of Recommendations for increasing the level of maturity of selected cyber security domains and subdomains according to the **NIST Cybersecurity Framework** based on the results obtained in Steps 1 and 2 Step 3.2 – Development of templates of necessary documents (including, but not limited to, policies, procedures, instructions) Step 3.3 – Determining the resources required to implement the Recommendations developed in Step 3.1 and the documents developed in Step 3.2 (including, but not limited to, time, personnel, equipment) Step 3.4 – Development of a report based on the results of Stage 3 Step 3.5 – Agreement with the Recipient and the Activity of the Report based on the results of Stage 3.	**Етап 3 – Розробка Рекомендацій для набуття цільового рівня зрілості кібербезпеки Реципієнта відповідно NIST Cybersecurity Framework** Крок 3.1 – Розробка Рекомендацій для підвищення рівня зрілості обраних доменів та субдоменів кібербезпеки **NIST Cybersecurity Framework**, на основі результатів отриманних на Етапах 1 та 2 Крок 3.2 – Розробка шаблонів необхідних документів (включаючи, та не обмежуючись - політик, процедур, інструкцій) Крок 3.3 – Визначення ресурсів необхідних для впровадження Рекомендацій розроблених на Кроці 3.1 та документів, розроблених на Кроці 3.2 (включаючи, але не обмежуючись - час, персонал, обладнання) Крок 3.4 – Розробка звіту за результатами Етапу 3 Крок 3.5 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 3.
Stage 4 - Development of the Roadmap for the implementation of the Recommendations for the acquisition of the target level of the Recipient's cybersecurity maturity in accordance with the NIST Cybersecurity Framework Step 4.1 – Development of a 4-month Roadmap for the implementation of the developed Recommendations, based on the results of Stage 3 and, but not limited to, interviews and discussions with stakeholders from the Recipient side Step 4.2 – Developing a report based on the results of Stage 4 and filling in the Recommendation Plan tab (План впровадження рекомендацій) of the spreadsheet (Forma_Daignostyky_OKI.xlsm file) provided by the Activity and completed by the Contractor. The completed spreadsheet tab must be included in the Stage report. Step 4.3 – Agreement with the Recipient and the Activity of the Report based on the results of Stage 4	**Етап 4 – Розробка Дорожної Карти впровадження Рекомендацій для набуття цільового рівня зрілості кібербезпеки Реципієнта відповідно до NIST Cybersecurity Framework** Крок 4.1 – Розробка 4-місячної Дорожньої Карти впровадження розроблених Рекомендацій, на основі результатів Етапу 3 та, але не обмежуючись, інтерв'ю та обговореннями зі стейкхолдерами зі сторони Рецепієнта Крок 4.2 – Розробка звіту за результатами Етапу 4 та заповнення вкладки Recommendation Plan (План впровадження рекомендацій) електронної таблиці (файл Forma_Daignostyky_OKI.xlsm), що надає Замовник та заповнює Підрядник. Заповнена вкладка електронної таблиці повинна бути включена до звіту за Етап. Крок 4.3 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 4

Stage 5 – Consultative and methodological support of the Recipient at the stage of implementation of the Road Map Recommendations Step 5.1 – Provision of monthly advisory support (to the Recipient by the Contractor at the stage of implementation of the Recommendations obtained as a result of Stage 3 and the Road Map obtained as a result of Stage 4 Step 5.2 – Monitoring by the Contractor of the progress of the implementation of the Recommendations by the Recipient on a monthly basis within the framework of the schedule determined by the Road Map based on the results of Stage 4 Step 5.3 – Submission of a monthly report within 6 months of the implementation of the Recommendations provided as a result of Stage 3 and the Road Map, describing the Recipient's progress and identified problems and backlogs (if any) Step 5.4 – Agreement with the Activity of monthly reports based on the results of Stage 4. **Stage 6 – Re-diagnostics to confirm the Recipient's achievement of the target cybersecurity maturity level according to the NIST Cybersecurity Framework** Step 6.1 - Gather information on the current state of cybersecurity of NIST Cybersecurity Framework domains and subdomains identified in Step 2 as high priority for Improvement - information may be obtained including, but not limited to, conducting interviews with interested Recipient representatives, collection of documentary evidence - "artifacts" (acts, procedures, policies, downloads of software settings, contracts, regulatory documents, screenshots) Step 6.2 – Analysis of the information collected in Step 6.1 for compliance with the requirements of the cyber security domains and subdomains of the NIST Cybersecurity Framework – the analysis should include a description of the procedure for checking compliance with the requirements of each subdomain and providing evidence (artifacts) used. Step 6.3 - Based on the information analyzed in Step 6.2, determine the confirmation of the Recipient's achievement of the target level of cybersecurity maturity in accordance with the NIST Cybersecurity Framework - the analysis should include a description of the procedure for checking	**Етап 5 – Консультативно-методологічна підтримка Реципієнта на етапі впровадження Рекомендацій за Дорожньою Картою** Крок 5.1 – Надання щомісячної консультативної підтримки Реципієнта Підрядником на етапі впровадження Рекомендацій отриманих за результатами Етапу 3 та Дорожньої Карти отриманої за результатами Етапу 4 Крок 5.2 – Відслідковування Підрядником прогресу впровадження Рекомендацій Реципієнтом на щомісячній основі в рамках графіку визначеного Дорожньою Картою за результатами Етапу 4 Крок 5.3 – Надання щомісячного звіту протягом 6 місяців впровадження Рекомендацій наданих за результатами Етапу 3 та Дорожної Карти з описом прогресу Реципієнта та виявлених проблем та відставань (за наявності) Крок 5.4 – Погодження з Замовником щомісячних Звітів за результатами виконання Етапу 4. **Етап 6 – Повторна діагностика для підтвердження досягнення Реципієнтом цільового рівня зрілості кібербезпеки згідно NIST Cybersecurity Framework** Крок 6.1 – Збір інформації про поточний стан кібербезпеки доменів та субдоменів NIST Cybersecurity Framework, що були визначені на Етапі 2, як першочергові для Покращення – інформація може бути отримана у тому числі, але не обмежуючись – з проведення інтерв'ю з зацікавленими представниками Реципієнта, збір документальних доказів – «артефактів» (актів, процедур, політик, вивантажень налаштувань програмного забезпечення, договорів, нормативних документів, знімків екранів) Крок 6.2 – Аналіз зібраної на Кроці 6.1 інформації на відповідність вимогам доменів та субдоменів кібербезпеки NIST Cybersecurity Framework – аналіз повинен включати в себе опис процедури перевірки на відповідність вимогам кожного субдомена та наведенням використаних доказів (артефактів) Крок 6.3 – На основі проаналізованої на Кроці 6.2 інформації визначення підтвердження досягнення Реципієнтом цільового рівня зрілості кібербезпеки у відповідності з NIST Cybersecurity Framework – аналіз повинен включати в себе опис процедури перевірки на відповідність вимогам кожного субдомена та

compliance with the requirements of each subdomain and providing evidence (artifacts) used. The maturity level is determined as follows - each subcategory is evaluated on a scale from 1 to 5 points (0 level - 0 points, 1 level - 1 point, 2 level - 2 points, 3 level - 3 points, 4 level - 4 points, the point is assigned in that case - if the sub-domain fully meets the requirements of the maturity level level), after which if 0 to 107 points are scored - it is 0 level for the organization as a whole, from 108 to 215 - 1 level, from 216 to 323 - 2 level, from 324 to 431 – 3 level, 432– 4 level). All points are included when filling (Re-diagnostics tab) into the spreadsheet (Forma_Diagnostyky_OKI.xlsm file) provided by the Activity and filled by the Contractor. Step 6.4 – Preparation of a report based on the results of Step 6, which includes a completed table based on the results of Step 6.3 Step 6.5 – Agreement with the Recipient and the Activity of the Report based on the results of Stage 6.	наведенням використаних доказів (артефактів). Визначення рівня зрілості відбувається наступним чином – кожна субкатегорія оцінюється по шкалі від 1 до 5 балів (0 рівень – 0 балів, 1 рівень – 1 бал, 2 рівень – 2 бали, 3 рівень - 3 бали, 4 рівень – 4 балів, бал присвоюється в тому випадку – якщо субдомен повністю відповідає вимогам рівня зрілості), після чого якщо набрано від 0 до 107 балів – це 0 рівень для організації в цілому, від 108 до 215 – 1 рівень, від 216 до 323 – 2 рівень, від 324 до 431 – 3 рівень, 432– 4 рівень). Всі бали включаються при заповненні (вкладка Re-diagnostics (Повторна діагностика) до електронної таблиці (файл Forma_Diagnostyky_OKI.xlsm),, що надає Замовник та заповнює Підрядник. Крок 6.4 – Підготовка звіту за результатами Етапу 6, що включає в себе заповнену таблицю за результатами Кроку 6.3 Крок 6.5 – Погодження з Реципієнтом та Замовником Звіту за результатами Етапу 6

Attachment B: Proposal Cover Letter/ Додаток В Супровідний лист

We, the undersigned, provide the attached proposal in accordance RFP No. REQ-_____ dated _____, 2023. 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:

Email:

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-_____ від _____ 2023 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 уповноваженної особи:

Ім’я та посада уповноваженної особи:

Назва організації:

Адреса:

Телефон:

Email:

Печатка компанії:

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

Item Number	Item Name Назва	Description/Specifications Опис/Специфікації	Quantity Кількість	Unit Price Ціна за од	Total Price Всього
1					
2					
3					
4					
5					
6					
7					
GRAND TOTAL IN UAH.					
GRAND TOTAL IN UNITED STATES DOLLARS					$

Delivery Period: Click here to enter text.

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

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

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

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

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

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

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

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

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.

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 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»

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 U.S. 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.

Summary of Previous U.S. Government Requirements – DUNS

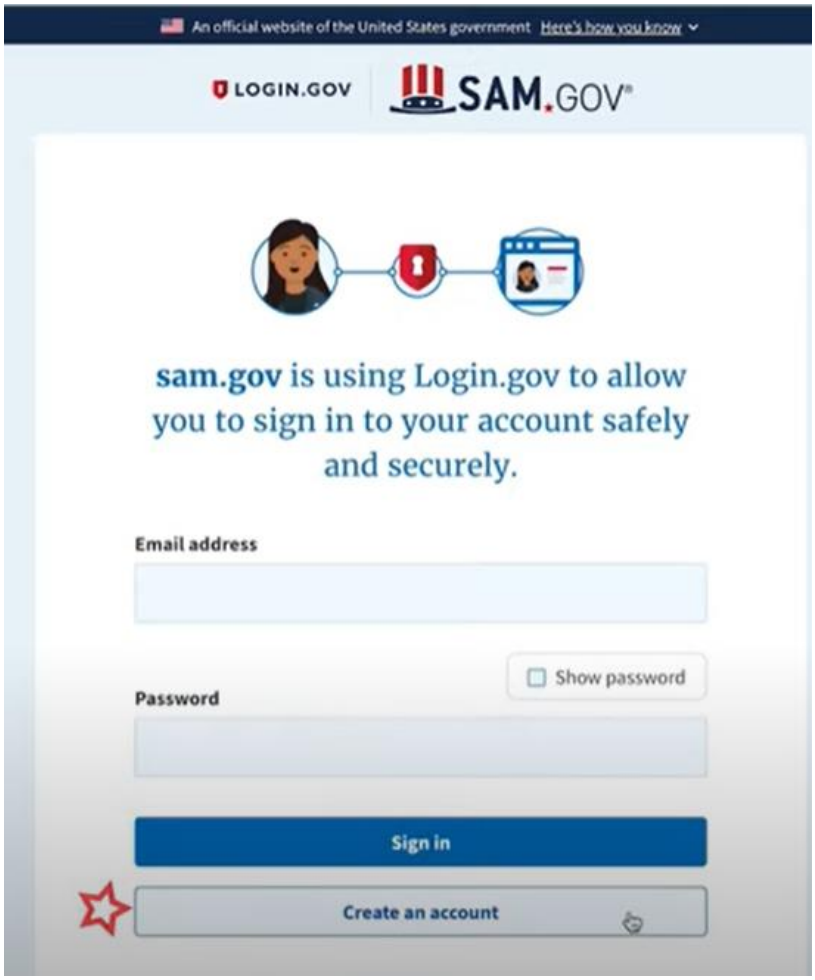
The Data Universal Numbering System (DUNS) is a system developed and managed by Dun and Bradstreet that assigns a unique nine-digit identifier to a business entity. It is a common standard world-wide and was previously used by the U.S. Government to assign unique entity identifiers. This system was retired by the U.S. 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), an 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 in order to obtain an Unique Entity ID (SAM) for your organization begin on the next page.

THE PROCESS FOR OBTAINING AN UNIQUE ENTITY ID IS OUTLINED BELOW:

1. Have the following information ready to request an Unique Entity ID (SAM)
    a. Legal Business Name
    b. Physical Address (including ZIP + 4)
    c. SAM.gov account (this is a user account, not actual SAM.gov business registration).
        i. **As a new user**, to get a SAM.gov account, go to www.sam.gov.
            1. Click "Sign In" on the upper right hand corner.
            2. Click on "Create a User Account"

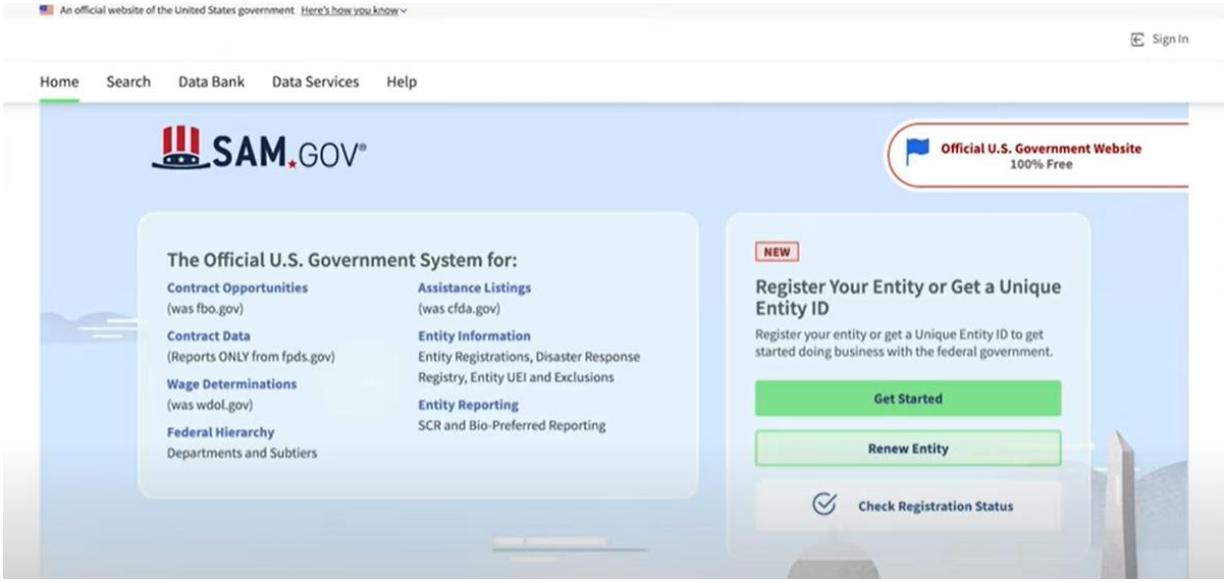


3. Choose Account Type:
    a. Create an Individual User Account to perform tasks such as register/update your entity, create and manage exclusion records or to view FOUO level data for entity records.
    b. Create a System User Account if you need system-to-system communication or if performing data transfer from SAM to your government database system. Complete the requested information, and then click "Submit."
4. Click "DONE" on the confirmation page. You will receive an email confirming you have created a user account in SAM.
5. Click the validation link in the email that contains the activation code within 48 hours to activate your user account. If the email link is not hyperlinked (i.e.,

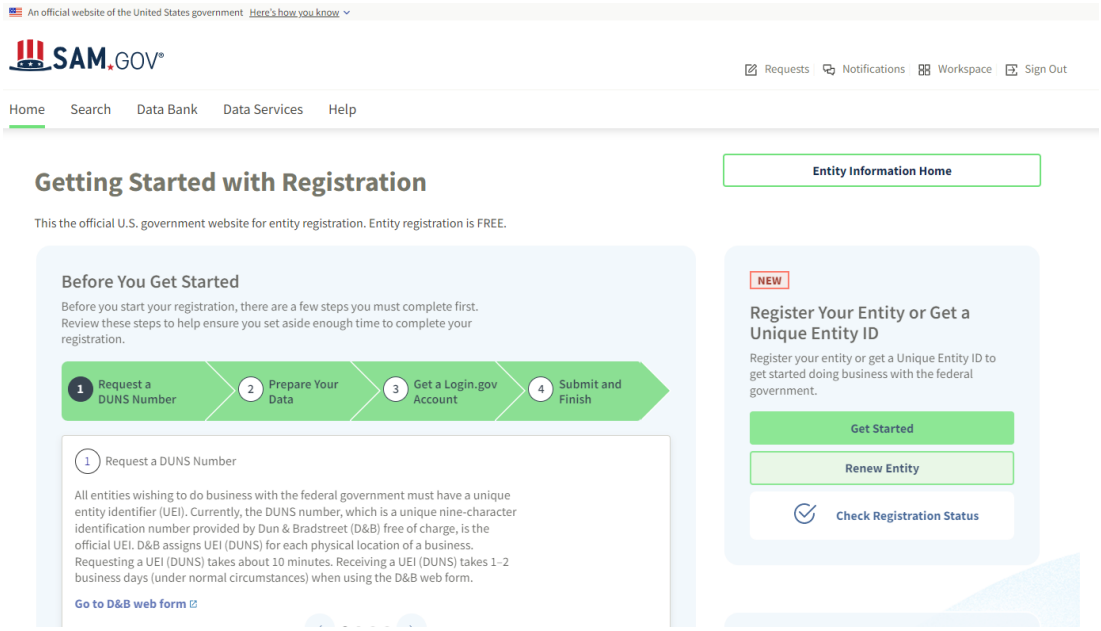
underlined or appearing in a different color), please copy the validation link and paste it into the browser address bar. You can now register an entity.

NOTE: Creating a user account does not create a registration in SAM, nor will it update/renew an existing registration in SAM.

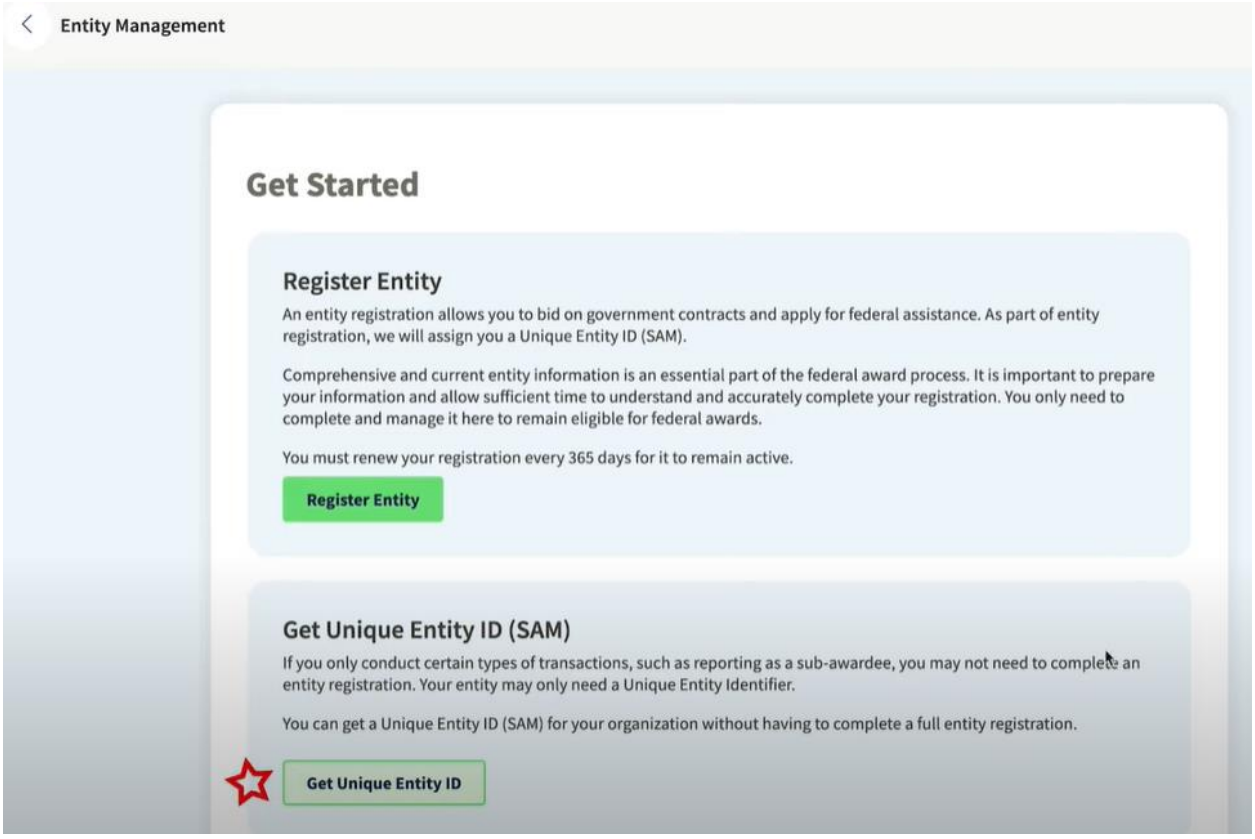
2. Once you have registered as a user, you can get an Unique Entity ID by selecting the "Get Started" button on the SAM.gov home page.



3. Select "Get Started" on the Getting Started with Registration page.



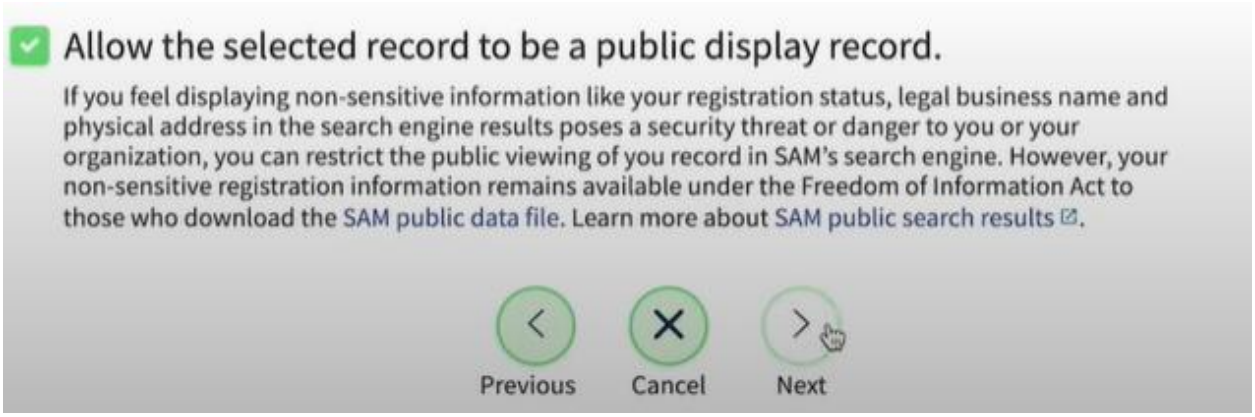
4. Select "Get Unique Entity ID" on the Get Started page.



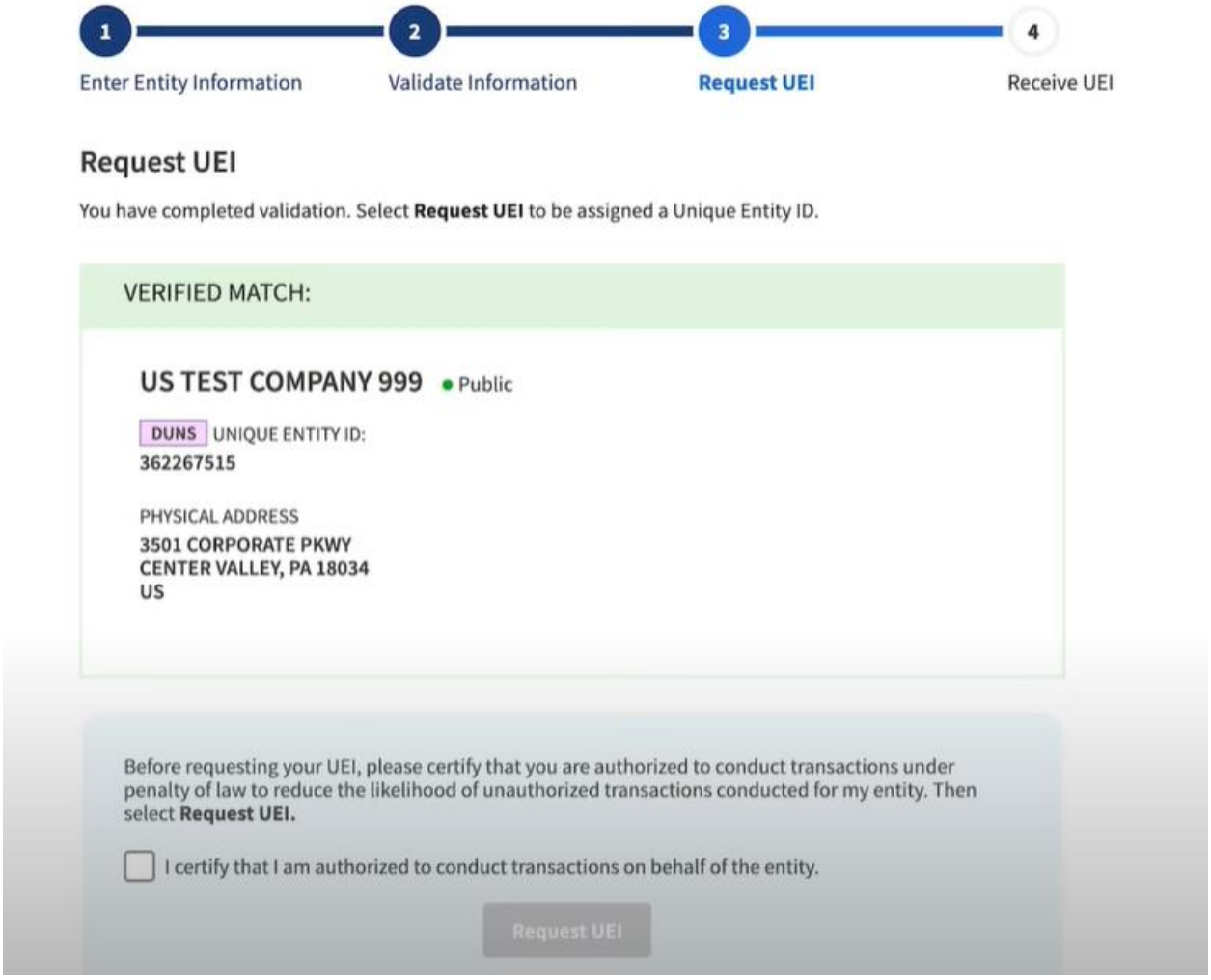
5. Enter Entity Information.

   a. If you previously had a DUN Number, make sure your Legal Business Name and Physical Address are accurate and match the Entity Information, down to capitalization and punctuation, used for DUNS registration.
6. When you are ready, select “Next”
7. Confirm your company’s information.

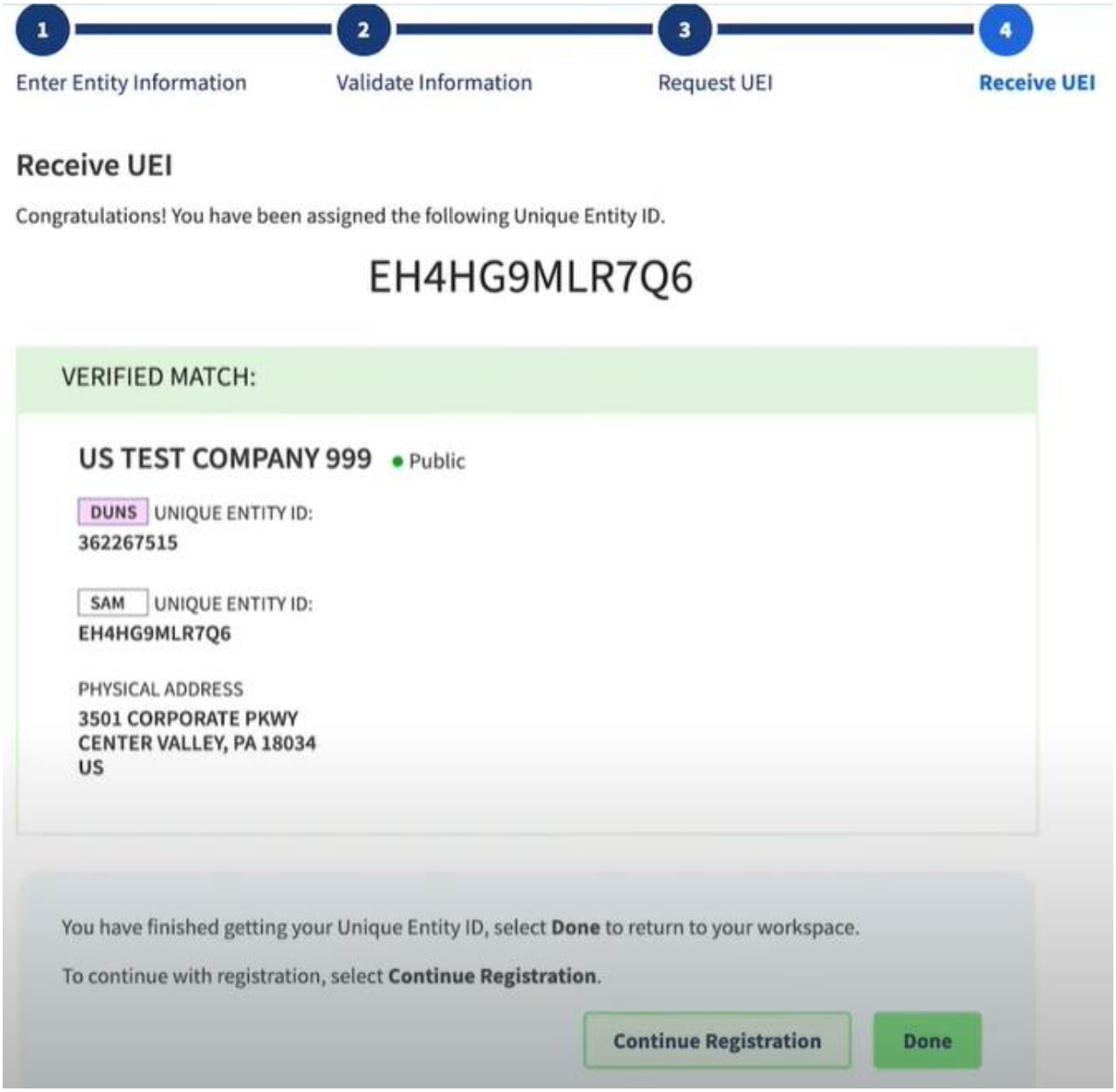
   a. On this page you will have the option to restrict the public search of this information. “Allow the selected record to be a public display record.” If you uncheck this box, only you and the federal government users will be able to search and view the entity information and entities like DAI will not be able to independently verify that you have an Unique Entity Identifier (SAM).



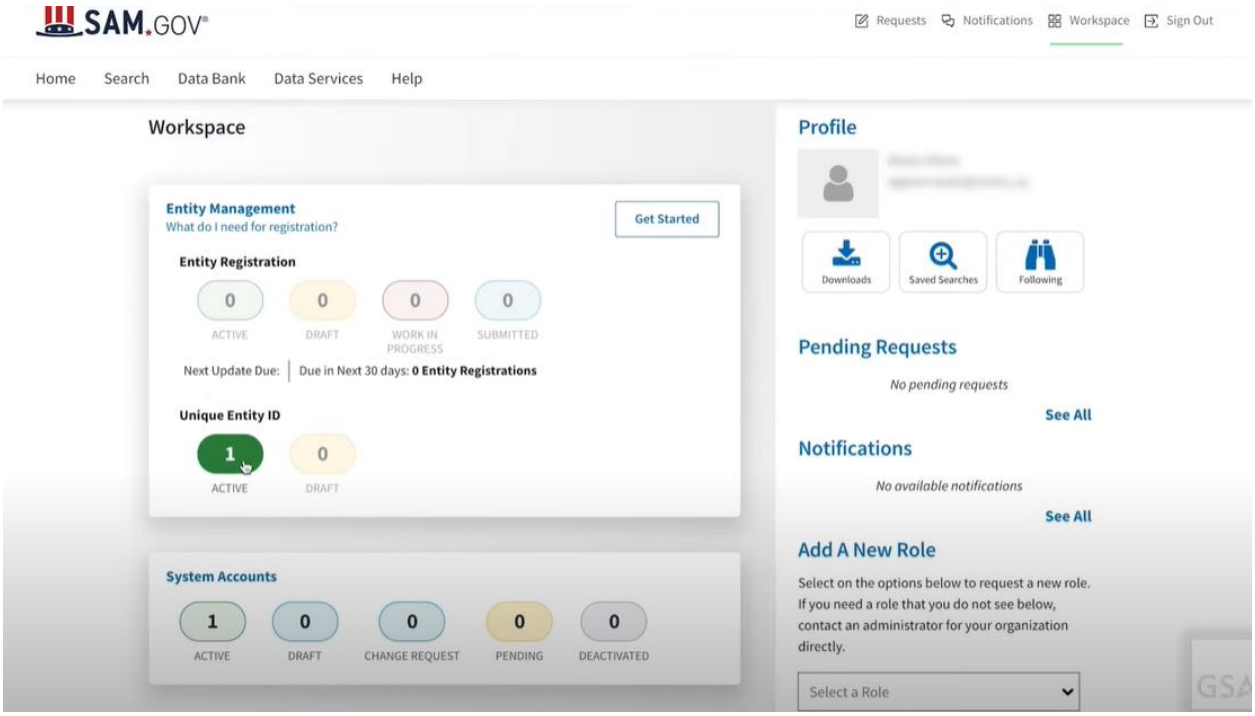
8. When you are ready, select "Next"
9. Once validation is completed, select "Request UEI" to be assigned an Unique Entity ID (SAM). Before requesting your UEI (SAM), you must certify that you are authorized to conduct transactions under penalty of law to reduce the likelihood of unauthorized transactions conducted for the entity.



10. The Unique Entity ID will be shown on the next page. SAM.gov will send an email confirmation with your Unique Entity ID.



11. If you need to view the Unique Entity ID from SAM in the future or update the organization's information, sign into SAM.gov and go to "Entity Management" widget.



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.

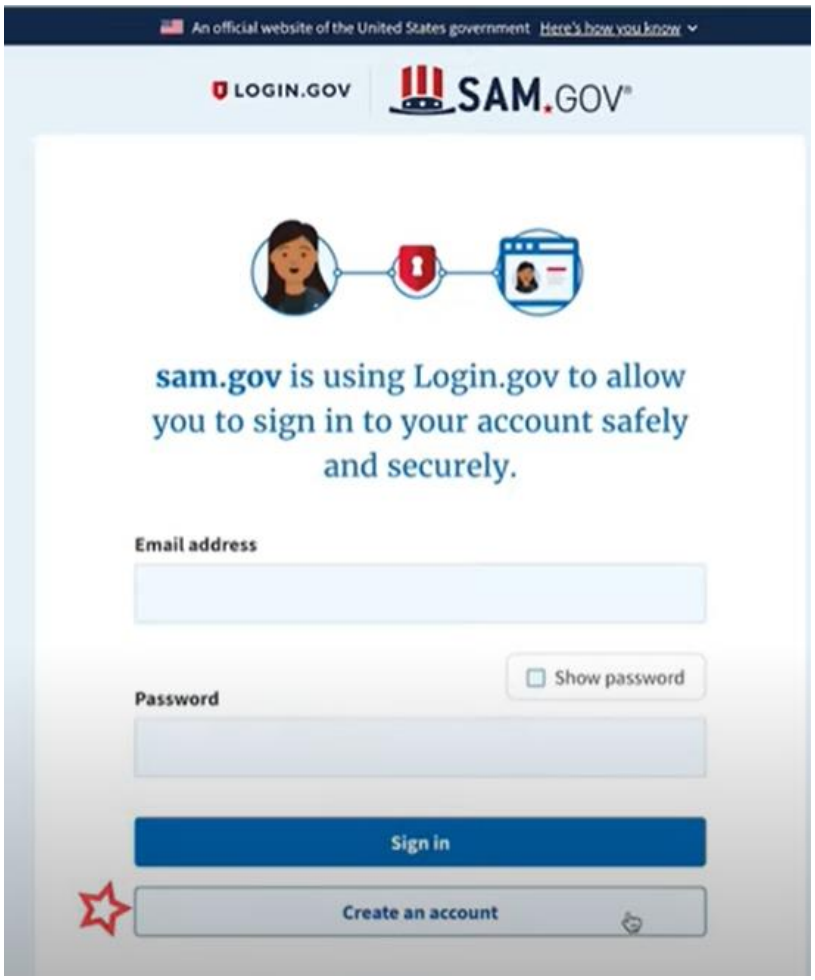
Стислий огляд колишніх вимог уряду США – DUNS

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.

ПРОЦЕС ОТРИМАННЯ УНІКАЛЬНОГО ІДЕНТИФІКАТОРА ЮРИДИЧНОЇ ОСОБИ ОПИСАНО НИЖЧЕ:

1. Щоб подати запит на отримання унікального ідентифікатора юридичної особи (SAM), підготуйте таку інформацію:
    a. Юридична назва підприємства
    b. Фізична адреса (включаючи поштовий індекс + 4)
    c. Обліковий запис на сайті SAM.gov (це обліковий запис користувача, а не фактична реєстрація підприємства на SAM.gov).
        i. **Якщо ви новий користувач:** щоб створити обліковий запис на сайті SAM.gov, перейдіть за посиланням: www.sam.gov.
            1. Натисніть «Увійти / Sign In» у верхньому правому куті.
            2. Натисніть «Створити обліковий запис користувача / Create a User Account».

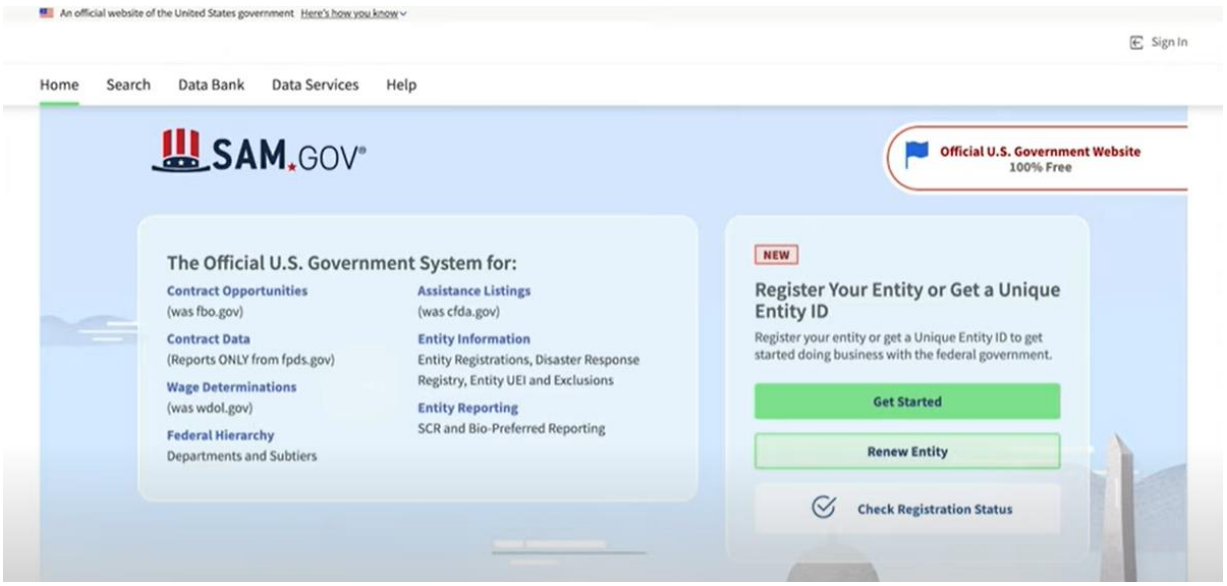


3. Виберіть тип облікового запису:
    a. Створіть обліковий запис індивідуального користувача, щоб виконувати такі завдання, як реєстрація / оновлення даних щодо вашої організації, створення записів та управління записами про виключення або перегляд даних рівня «для службового користування» стосовно організації.

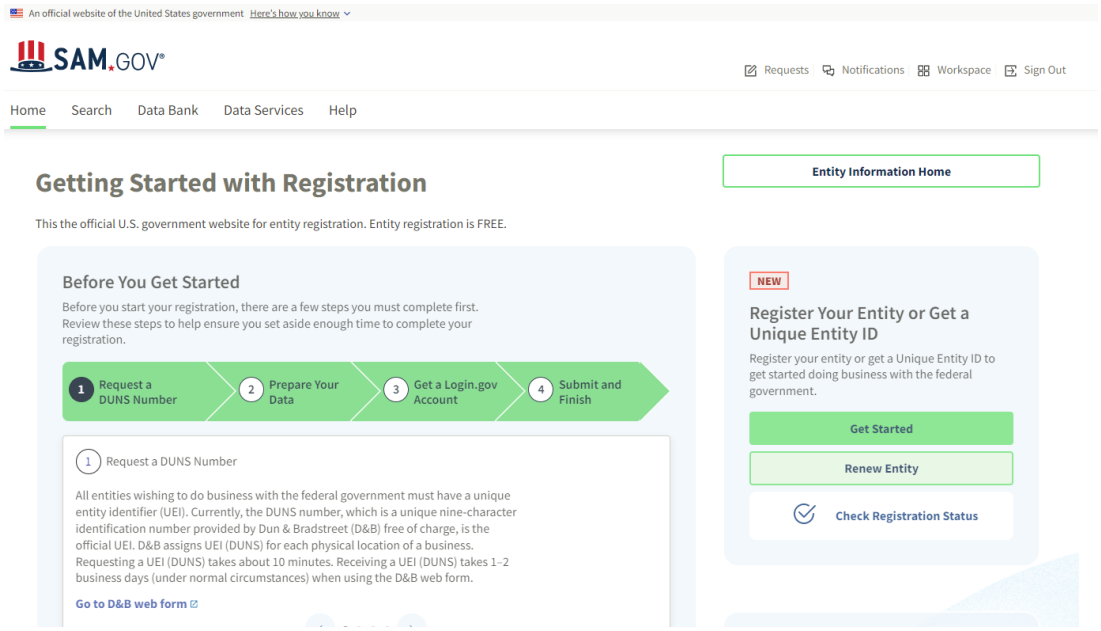
    b. Створіть обліковий запис системного користувача, якщо вам потрібно встановити зв'язок між системами або якщо ви виконуєте передання даних із SAM до вашої урядової системи баз даних. Введіть потрібну інформацію і натисніть «Подати / Submit».

4. Натисніть «ГОТОВО / DONE» на сторінці підтвердження. Ви одержите електронний лист із підтвердженням створення облікового запису користувача в системі SAM.
5. Перейдіть за посиланням із кодом активації в електронному листі впродовж 48 годин, щоб активувати обліковий запис користувача. Якщо посилання в листі не є гіперпосиланням (тобто підкресленим або виділеним іншим кольором), скопіюйте посилання і вставте його в адресний рядок браузера. Тепер ви можете зареєструвати організацію.
   ПРИМІТКА: Створення облікового запису користувача не приводить до створення реєстрації в SAM або до оновлення/продовження наявної реєстрації в SAM.

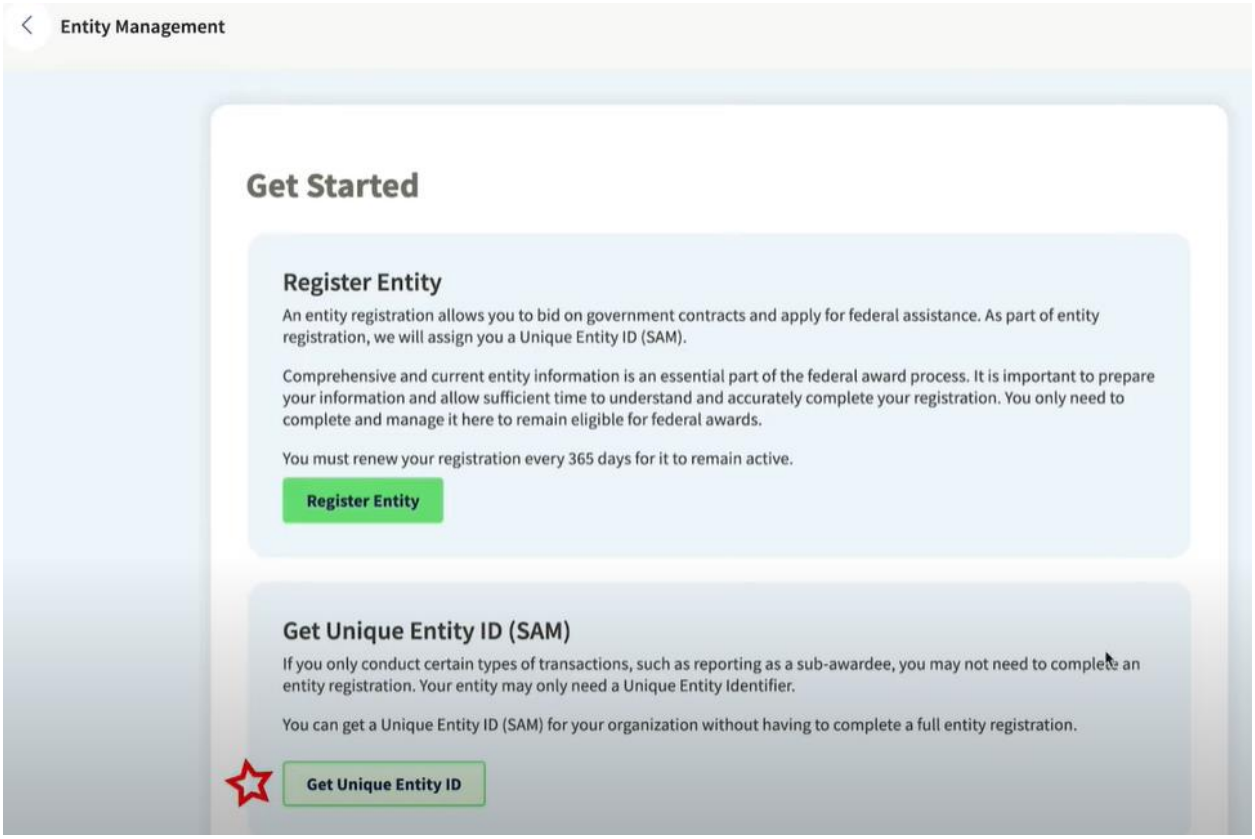
2. Після своєї реєстрації як користувача ви можете отримати унікальний ідентифікатор юридичної особи, вибравши кнопку «Почати / Get Started» на головній сторінці SAM.gov.



3. Виберіть «Почати / Get Started» на сторінці «Початок реєстрації / Getting Started with Registration».



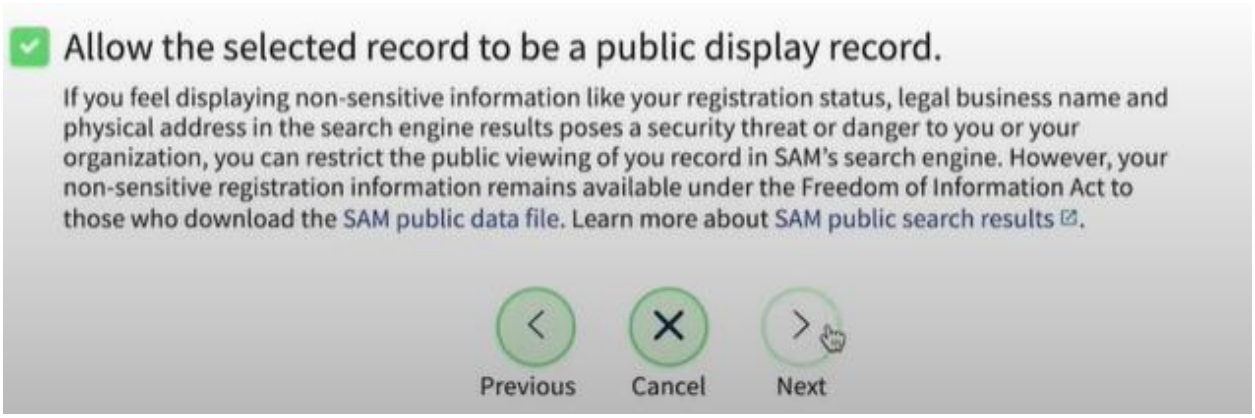
4. Виберіть «Отримати унікальний ідентифікатор юридичної особи / Get Unique Entity ID» на сторінці «Почати / Get Started».



5. Введіть інформацію про юридичну особу.

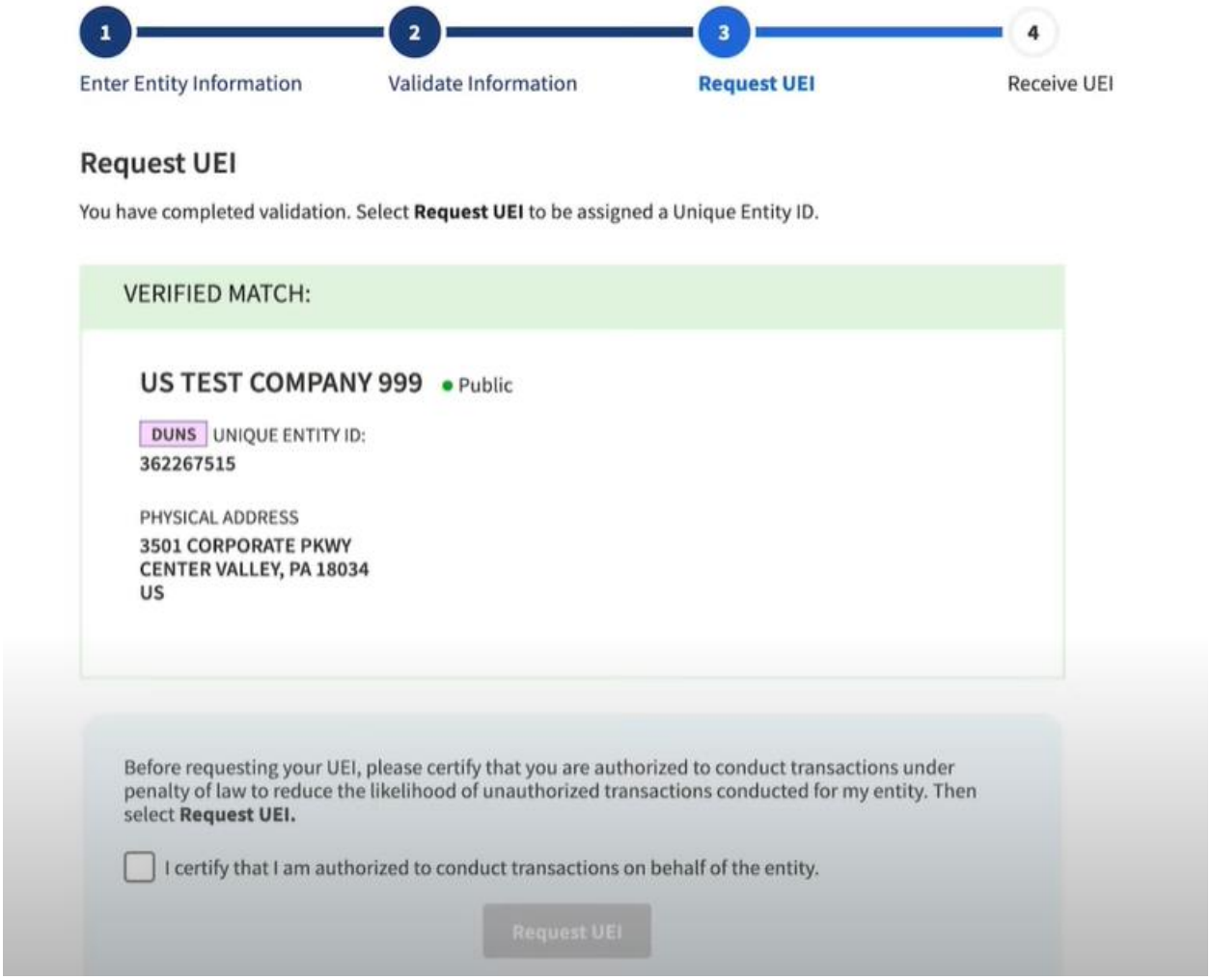
   a. Якщо у вас раніше був номер DUNS, переконайтеся, що юридична назва та фізична адреса вашого підприємства є точними і відповідають інформації про юридичну особу, аж до великих літер та пунктуації, що використовувалася під час реєстрації в DUNS.
6. Коли будете готові, виберіть «Далі / Next».
7. Підтвердьте інформацію про вашу компанію.

   a. На цій сторінці ви можете обмежити доступність цієї інформації для публічного пошуку. «Дозволити публічне відображення вибраного запису / Allow the selected record to be a public display record». Якщо ви знімете цей прапорець, лише ви і представники федерального уряду зможуть шукати і переглядати інформацію про компанію, тоді як такі організації, як DAI, не зможуть самостійно перевірити наявність у вас унікального ідентифікатора юридичної особи (SAM).



8. Коли будете готові, виберіть «Далі / Next».

9. Після завершення перевірки виберіть «Запит унікального ідентифікатора / Request UEI», щоб отримати унікальний ідентифікатор юридичної особи (SAM). Перш ніж подавати запит на отримання унікального ідентифікатора юридичної особи (SAM), ви повинні засвідчити (пам'ятаючи про покарання, передбачене законом), що уповноважені проводити операції. Це потрібно, щоб зменшити ймовірність несанкціонованих операцій стосовно організації.



Attachment F: Self-Certification for Exemption from SAM Requirement/ Додаток F: Форма самовизначення на звільнення від вимоги отримання SAM номеру

Legal Business Name:/ Назва компанії:	
Physical Address:/ Фізична адреса:	
Physical City:/ Місто:	
Physical Foreign Province (if applicable):/ Регіон (якщо застосовується):	
Physical Country:/ Країна:	
Signature of Certifier/ Підпис заявника:	
Full Name of Certifier (Last Name, First/Middle Names):/ Повне ім'я заявника (прізвище, ім'я, по батькові/середнє ім'я:	
Title of Certifier:/ Посада заявника:	
Date of Certification (mm/dd/yyyy):/ Дата заяви (мм.дд.рррр):	

The sub-contractor/vendor whose legal business name is provided herein, certifies that we are an organization exempt from obtaining a SAM number, as the gross income received from all sources in the previous tax year is under USD $300,000.
Субпідрядник/постачальник, указаний у цій заяві, цим заявляє, що є організацією, яка підлягає звільненню від вимоги отримання номера SAM, оскільки її валовий дохід, отриманий із усіх джерел за попередній податковий рік, був нижче 300 000 доларів США.

*By submitting this certification, the certifier attests to the accuracy of the representations and certifications contained herein. The certifier understands that s/he and/or the sub-contractor/vendor may be subject to penalties, if s/he misrepresents the sub-contractor/vendor in any of the representations or certifications to the Prime Contractor and/or the US Government.
The sub-contractor/vendor agrees to allow the Prime Contractor and/or the US Government to verify the company name, physical address, or other information provided herein. Certification validity is for one year from the date of certification.
* Подаючи цю заяву, заявник підтверджує достовірність поданої в ній інформації. Заявник розуміє, що до нього/неї та/або субпідрядника/ постачальника можуть бути застосовані санкції, якщо він/вона неправильно представить заяви або підтвердження субпідрядника/ постачальника генеральному підряднику та/або Уряду США.

Субпідрядник/ постачальник погоджується дозволити генеральному підряднику та/або Уряду США перевіряти назву, фізичну адресу або інші дані про компанію, наведені в цій заяві. Ця заява дійсна протягом року із дати її видачі.

Attachment G: Past Performance/ Додаток G: Досвід роботи

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

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

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

Attachment H: Information about CIO/ Додаток H: Інформація про ОКІ

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

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

Name of CIO / Назва ОКІ	Public joint-stock company "National Depository of Ukraine" / Публічного акціонерного товариства «Національний Депозитарій України»
Official Website / Офіційний Веб-сайт	https://www.csd.ua/
Number of employees / Кількість працівників	90
Number of main divisions (departments) / Кількість основних структурних підрозділів (департаментів)	10
Number of regional offices / Кількість регіональних представництв	0
The number of informational systems, administrated or managed by CIOs / Кількість інформаційних систем, адміністраторами або розпорядниками яких є ОКІ	25