Request for Proposal (RFP)

USAID Cybersecurity for Critical Infrastructure (USAID Cybersecurity)

REQ-KYI-21-0294

Procurement of Threat Intelligence Platform (TIP)

Issued by: DAI Global, LLC

Issue Date: July 14, 2021

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 to ensure amendments to the RFP or other communications are sent directly to them. Any prospective Offeror who fails to express 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 by email.

Contents

Synopsis of the Request for Proposals (RFP)

RFP No.	REQ-KYI-21-0294
Issue Date	**July 14, 2021**
Title	Procurement of Threat Intelligence Platform (TIP)
Email Address for Submission of Proposals	Proposals should be submitted to UkraineCCI_Proposals@dai.com
Deadline for Receipt of Questions	**July 26, 2021**, **18:00**, Kyiv, 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.
Deadline for Receipt of Proposals	**July 30, 2021, 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**
Point of Contact	UkraineCCI_Procurement@dai.com
Anticipated Award Type	**Firm Fixed Price Purchase Order** – is a commercial document issued by a buyer to a vendor indicating types, quantities, and agreed prices for products or services. Issuance of this RFP in no way obligates DAI to award purchase order or subcontract and offerors will not be reimbursed for any costs associated with the preparation of their bid.
Basis for Award	An award will be made based on the **Trade Off Method**. The award will be issued to the responsible and reasonable offeror 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 "Responsibility Determination".

Introduction and Purpose

Purpose

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the Activity) is a program funded by USAID and implemented by DAI along with implementing partners Catalisto, Florida International University (FIU), Information Systems Security Partners (ISSP), Schweitzer Engineering Laboratories (SEL), SocialBoost, and Veterans First Initiative (VFI). 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 four-year period, the Activity will increase resilience and build capacity to prevent, detect, and respond to cyberattacks against critical infrastructure 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 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.

Under the enabling environment component, the Activity is implementing interventions in partnership with cybersecurity stakeholders in Ukraine aimed at increasing national preparedness for responding to cybersecurity threats and attacks, particularly those aimed at CI sectors. As part of this effort, the Activity is also collaborating with stakeholders to develop a comprehensive Threat Intelligence Sharing Mechanism (TISM), an important step in improving cybersecurity resilience through improved threat intelligence sharing. The model proposed by the Activity and its partners allows for multiple intelligence sharing platforms or services to connect based on open standards, such as STIX/TAXII1 and shared protocols. In support of this model, the Activity is seeking the provision of a Threat Intelligence Platform (TIP), a technology that helps organizations collect, aggregate, and analyze threat data from multiple sources and formats in real time. Within the Activity's TISM plan, the proposed TIP will allow

[1] Structured Threat Information eXpression/Trusted Automated Exchange of Intelligence Information

information related to cyber threats to be securely and appropriately collected by and shared between and across relevant Government of Ukraine (GOU) entities and CI operators. At a minimum, the TIP must be able to:

1) Collect and aggregate threat intelligence data from across organizations and diverse sources,
2) Integrate organizations' existing tools and systems
3) Allow analysis and sharing of intelligence data across stakeholders/recipient organizations and existing threat intelligence systems/platforms
4) Normalize and enrich data

Issuing Office

The Issuing Office noted in the above synopsis is the sole point of contact at DAI for purposes of this RFP. Any prospective Offeror who fails to express their interest to this office assumes complete responsibility in the event that they do not receive direct communications (amendments, answers to questions, etc.) prior to the closing date.

Type of Award Anticipated

DAI anticipates awarding a **Firm Fixed Price Purchase Order**. This subcontract type is subject to change during the course of negotiations.

General Instructions to Offerors

General Instructions

"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 to propose the work.

Offerors wishing to respond to this RFP must submit proposals, in English, in accordance with the following 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.

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.

Proposals are due no later than**, July 30, 2021**, **18:00, Kyiv, Ukraine Time**, to be submitted via procurement email UkraineCCI_Proposals@dai.com. **The RFP number and title of the activity must be stated in the subject line of the email.** Cost and technical proposals shall be submitted to the same mailbox in ***two different files*** (VOLUME I: TECHNICAL PROPOSAL and VOLUME II: COST/PRICE PROPOSAL). Late offers will be rejected except under extraordinary circumstances at DAI's discretion.

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.

Proposal Cover Letter

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 **sixty (60) calendar days** for the prices provided.
- Acknowledge the solicitation amendments received.

Questions regarding the RFP

Each Offeror is responsible for reading and complying with the terms and conditions of this RFP. Requests for clarification or additional information must be submitted in writing via email or in writing to the Issuing Office as specified in the Synopsis above. No questions will be answered by phone. Any verbal information received from a DAI or (insert Project Acronym) employee or other entity shall not be considered as an official response to any question regarding this RFP.

Copies of questions and responses will be distributed in writing to all prospective bidders who are on record as having received this RFP after the submission date specified in the Synopsis above.

Instructions for the Preparation of Technical Proposals

Technical proposals shall be submitted by email separately from cost/price proposals and shall be clearly titled **"VOLUME I: TECHNICAL PROPOSAL"**.

Technical proposals shall include the following contents

1. Technical Approach - Description of the proposed services which meets or exceeds the stated technical specifications or scope of work. The proposal must show how the Offeror plans to complete the work and describe an approach that demonstrates the achievement of timely and acceptable performance of the work.

2. Management approach – Description of the Offeror's staff assigned to the project. The proposal should describe how the proposed team members have the necessary experience and capabilities to carry out the Technical Approach.
3. Past Performance –Provide a list of at least three (3) recent awards of similar scope and duration. The information shall be supplied as a table, and shall include the legal name and address of the organization for which services were performed, a description of work performed, the duration of the work and the value of the contract, description of any problems encountered and how it was resolved, and a current contact phone number of a responsible and knowledgeable representative of the organization. See Attachment F.

Services Specified

For this RFP, DAI is in need of the services described in Attachment A.

Technical Evaluation Criteria

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 other than cost/price, when combined, are considered approximately equal to cost/price factors.

Technical Approach	• Does the vendor actively develop and maintain API and connectors to other vendor products/hardware sensors? • Does the product provide flexible data models based on STIX2.X and MITRE ATT&CK standards? • Does the product provide the ability for internal and external data sources to be processed and stored as single data sets? • Does the product natively provide for on premises data storage? • Does the product and vendor support air-gapped deployments? • Does the product enable specific organizational data scoring attributes such as geographic and industry relevance? • Does the product automate expiration tasks based on source and indicator type data? • Does the product provide threat intelligence management features for generating, storing, collaborating and coordinating threat intelligence and actions/tasks? • Does the product provide the ability to log to and correlate data from disparate sources (e.g., SIEM)? • Does the proposal explain how the product can be sustainably maintained by customers?	40 points
Management Approach	• Does the proposal demonstrate the company's experience previously designed, developed, and supported a TIP solution for government agencies and/or state-owned enterprises? • Does the proposal demonstrate experience working in Ukraine or provided TIP solutions to Ukrainian clients?	30 points
Past Performance	• Does the proposal describe support and training provided with TIP? • Does the proposal describe expertise on the support team? • Does the proposal describe how the TIP will be deployed to stakeholders in Ukraine?	30 points
Total Points		100 points

Instructions for the Preparation of Cost/Price Proposals

Cost/Price Proposals

Cost/Price proposals shall be emailed separately 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 firm-fixed price awards. Offerors shall complete the template and submit supporting detail.

Basis of Award

Best Value Determination

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.**

Responsibility Determination

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 evidence of the required business licenses to operate in the host country.
2. Evidence of a DUNS number (explained below and instructions contained in Attachment D).
3. The source, origin and nationality of the products or services are not from a Prohibited Country (explained below).
4. Having adequate financial resources to finance and perform the work or deliver goods or the ability to obtain financial resources without receiving advance funds from DAI.
5. Ability to comply with required or proposed delivery or performance schedules.
6. Have a satisfactory past performance record.
7. Have a satisfactory record of integrity and business ethics.
8. Have the necessary organization, experience, accounting and operational controls and technical skills.
9. Have the necessary production, construction and technical equipment and facilities if applicable.
10. Be qualified and eligible to perform work under applicable laws and regulations.

Anticipated post-award Deliverables

Upon award of a subcontract, the deliverables and deadlines detailed in 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.

#	Deliverable/Product	Description
1	Trial of TIP	Fully functional trial license/subscription

2	TIP license	Provision of specific Platform license must be based on assessment (size of package, number of users, duration) of stakeholder/recipient organization, and include deployment services, role-appropriate and specific training for users, and ongoing technical support.

Inspection & Acceptance

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.

Compliance with Terms and Conditions

General Terms and Conditions

Offerors agree to comply with 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 G.

Source and Nationality

Under the authorized geographic code for its contract DAI may only procure goods and services from the following countries.

Geographic Code 937: Goods and services from the United States, the cooperating country, and "Developing Countries" other than "Advanced Developing Countries: excluding prohibited countries. A list of the "Developing Countries" as well as "Advanced Developing Countries" can be found at: ***http://www.usaid.gov/policy/ads/300/310maa.pdf*** and ***http://www.usaid.gov/policy/ads/300/310mab.pdf*** respectively.
Geographic Code 110: Goods and services from the United States, the independent states of the former Soviet Union, or a developing country, but excluding Prohibited Countries.

DAI must verify the source and nationality of goods and services and ensure (to the fullest extent possible) that DAI does not procure any goods or services from prohibited countries listed by the Office of Foreign Assets Control (OFAC) as sanctioned countries. OFAC sanctioned countries may be searched within the System for Award Management (SAM). The current list of countries under comprehensive sanctions include: Cuba, Iran, North Korea, Sudan, and Syria. Goods may not transit through or be assembled in comprehensive sanctioned origin or nationality countries nor can the vendor be owned or controlled by a prohibited country. 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 of the goods or services being offered and that the goods and services comply with the Geographic Code and the exclusions for prohibited countries outlined above.

Data Universal Numbering System (DUNS)

There is a **mandatory** requirement for your organization to provide a DUNS number to DAI. The Data Universal Numbering System is a system developed and regulated by Dun & Bradstreet (D&B) that assigns a unique numeric identifier, referred to as a "DUNS number" to a single business entity. Without a DUNS number, DAI cannot deem an Offeror “responsible” to conduct business with and therefore, DAI will not enter into a subcontract/purchase order or monetary agreement with any organization. The determination of a successful offeror/applicant resulting from this RFP/RFQ/RFA is contingent upon the winner providing a DUNS number to DAI. Offerors who fail to provide a DUNS number will not receive an award and DAI will select an alternate Offeror.

All U.S. and foreign organizations which receive first-tier subcontracts/ purchase orders with a value of $30,000 and above **are required** to obtain a DUNS 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 DUNS number, see Attachment D - Instructions for Obtaining a DUNS Number - DAI'S Vendors, Subcontractors

For those not required to obtain a DUNS number, see Attachment E: Self Certification for Exemption from DUNS Requirement

Procurement Ethics

Neither payment nor preference shall be made by either the Offeror, or by any DAI staff, in an attempt to affect the results of the award. DAI treats all reports of possible fraud/abuse very seriously. Acts of fraud or corruption will not be tolerated, and DAI employees and/or subcontractors/grantees/vendors who engage in such activities will face serious consequences. Any such practice constitutes an unethical, illegal, and corrupt practice and either the Offeror or the DAI staff may report violations to the Toll-Free Ethics and Compliance Anonymous Hotline at +1 855-603-6987, via the DAI website, or via email to FPI_hotline@dai.com. DAI ensures anonymity and an unbiased, serious review and treatment of the information provided. Such practice may result in the cancellation of the procurement and disqualification of the Offeror's participation in this, and future, procurements. Violators will be reported to USAID, and as a result, may be reported to the U.S. Department of Justice to be included in a Restricted Parties list, preventing them from participating in future U.S. Government business.

Offerors must provide full, accurate and complete information in response to this solicitation. The penalty for materially false responses is prescribed in Section 1001 of Title 18 of the United States Code.

In addition, DAI takes the payment of USAID funds to pay Terrorists, or groups supporting Terrorists, or other parties in exchange for protection very seriously. Should the Terrorist, groups or other parties attempt to extort/demand payment from your organization you are asked to immediately report the incident to DAI's Ethics and Compliance Anonymous Hotline at the contacts described in this clause.

By submitting an offeror, offerors certify that they have not/will not attempt to bribe or make any payments to DAI employees in return for preference, nor have any payments with Terrorists, or groups supporting Terrorists, been attempted.

Attachment A: Scope of Work for Services or Technical Specifications

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the Activity) is a program funded by USAID and implemented by DAI along with implementing partners Catalisto, Florida International University (FIU), Information Systems Security Partners (ISSP), Schweitzer Engineering Laboratories (SEL), SocialBoost, and Veterans First Initiative (VFI). 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 four-year period, the Activity will increase resilience and build capacity to prevent, detect, and respond to cyberattacks against critical infrastructure 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 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.

Under the enabling environment component, the Activity is implementing interventions in partnership with cybersecurity stakeholders in Ukraine aimed at increasing national preparedness for responding to cybersecurity threats and attacks, particularly those aimed at CI sectors. As part of this effort, the Activity is also collaborating with stakeholders to develop a comprehensive Threat Intelligence Sharing Mechanism (TISM), an important step in improving cybersecurity resilience through improved threat intelligence sharing. The model proposed by the Activity and its partners allows for multiple intelligence sharing platforms or services to connect based on open standards, such as STIX/TAXII[2] and shared protocols. In support of this model, the Activity is seeking the provision of a Threat Intelligence Platform

[2] Structured Threat Information eXpression/Trusted Automated Exchange of Intelligence Information

(TIP), a technology that helps organizations collect, aggregate, and analyze threat data from multiple sources and formats in real time. Within the Activity's TISM plan, the proposed TIP will allow information related to cyber threats to be securely and appropriately collected by and shared between and across relevant Government of Ukraine (GOU) entities and CI operators. At a minimum, the TIP must be able to:

1) Collect and aggregate threat intelligence data from across organizations and diverse sources,
2) Integrate organizations' existing tools and systems
3) Allow analysis and sharing of intelligence data across stakeholders/recipient organizations and existing threat intelligence systems/platforms
4) Normalize and enrich data

OBJECTIVE:

The TIP will support the TISM model in improving detection of and response to potential cybersecurity threats and attacks on critical infrastructure in Ukraine, promoting trust between cybersecurity stakeholders, and increasing interconnectedness at the national, sectoral and CI operator level.

TASKS:

The selected provider will be expected to:

- Assess stakeholder/recipient organization environment, including tools, workflows, etc.; Determine custom integrations required.
- Offer demos of appropriate TIP solutions based on stakeholder/recipient organizations' environment.
- Provide appropriate TIP solution for stakeholder/recipient organization.
- Provide services for deploying TIP for each stakeholder/recipient organization, ensuring integration with/into their existing environment/architecture.
- Provide adequate, focused and, as appropriate, role tailored, training on TIP usage for up to 14 stakeholder/recipient organization where TIP will be installed.
- Provide technical support for TIP customers, as needed.

TECHNICAL REQUIREMENTS:

The detailed technical specifications are provided in **Attachment I_Technical Requirements**.

DELIVERABLES:

See the detailed descriptions/specifications related to deliverables in Attachment C. Price Schedule.

Attachment B: Proposal Cover Letter

[On Firm's Letterhead]

<Insert date>

TO:

We, the undersigned, provide the attached proposal in accordance with **REQ-KYI-21-0294 Procurement of Threat Intelligence Platform (TIP)** issued on Click here to enter text..

Our attached proposal is for the total price of <Sum in Words ($0.00 Sum in Figures) >.

I certify a validity period of 60 (sixty) calendar days for the prices provided in the attached Price Schedule/Bill of Quantities. Our proposal shall be binding upon us subject to the modifications resulting from any discussions.

Offeror shall verify here the items specified in this RFP document.

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

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

Yours sincerely,

Authorized Signature:
Name and Title of Signatory: Click here to enter text.
Name of Firm: Click here to enter text.
Address: Click here to enter text.
Telephone: Click here to enter text.
Email: Click here to enter text.
Company Seal/Stamp:

Attachment C: Price Schedule

#	Product	Description	Quantity	Delivery date	Total price
1	Trial of TIP	Fully functional trial license/subscription	14		USD 0.00
2	TIP license	Provision of specific Platform license must be based on assessment (size of package, number of users, duration) of stakeholder/recipient organization, and include deployment services, role-appropriate and specific training for users, and ongoing technical support.	14		USD 0.00

Delivery Period: Click here to enter text.

Attachment D: Instructions for Obtaining a DUNS Number - DAI'S Vendors, Subcontractors

DUNS and SAM Registration Guidance

What is DUNS?
The Data Universal Numbering System (DUNS) is a system developed and regulated by Dun & Bradstreet (D&B) - a company that provides information on corporations for use in credit decisions - that assigns a unique numeric identifier, referred to as a DUNS number, to a single business entity. The DUNS database contains over 100 million entries for businesses throughout the world, and is used by the United States Government, the United Nations, and the European Commission to identify companies. The DUNS number is widely used by both commercial and federal entities and was adopted as the standard business identifier for federal electronic commerce in October 1994. The DUNS number was also incorporated into the Federal Acquisition Regulation (FAR) in April 1998 as the Federal Government's contractor identification code for all procurement-related activities.

Why am I being requested to obtain a DUNS number?
U.S. law – in particular the Federal Funding Accountability and Transparency Act of 2006 (Pub.L. 109-282), as amended by section 6202 of the Government Funding Transparency Act of 2008 (Pub.L. 110-252) - make it a requirement for all entities doing business with the U.S. Government to be registered, currently through the System for Award Management, a single, free, publicly - searchable website that includes information on each federal award. As part of this reporting requirement, prime contractors such as DAI Global LLC must report information on qualifying subawards as outlined in FAR 52.204-10 and 2CFR Part 170. DAI Global LLC is required to report subcontracts with an award valued at greater than or equal to $30,000 under a prime contract and subawards under prime grants or prime cooperative agreements obligating funds of $25,000 or more, whether U.S. or locally-based. Because the U.S. Government uses DUNS numbers to uniquely identify businesses and organizations, DAI Global LLC is required to enter subaward data with a corresponding DUNS number.

Is there a charge for obtaining a DUNS number?
No. Obtaining a DUNS number is absolutely free for all entities doing business with the Federal government. This includes current and prospective contractors, grantees, and loan recipients.

How do I obtain a DUNS number?
DUNS numbers can be obtained online at http://fedgov.dnb.com/webform/pages/CCRSearch.jsp or by phone at 1-800-234-3867 (for US, Puerto Rico and Virgin Island requests only).
(Also https://fedgov.dnb.com/webform)

What information will I need to obtain a DUNS number?
To request a DUNS number, you will need to provide the following information:

- Legal name and structure
- Tradestyle, Doing Business As (DBA), or other name by which your organization is commonly recognized
- Physical address, city, state and Zip Code
- Mailing address (if separate)
- Telephone number
- Contact name
- Number of employees at your location

- Description of operations and associated code (SIC code found at https://www.osha.gov/pls/imis/sicsearch.html)
- Annual sales and revenue information
- Headquarters name and address (if there is a reporting relationship to a parent corporate entity)

How long does it take to obtain a DUNS number?
Under normal circumstances the DUNS is issued within 1-2 business days when using the D&B web form process. If requested by phone, a DUNS can usually be provided immediately.
Are there exemptions to the DUNS number requirement?
There may be exemptions under specific prime contracts, based on an organization's previous fiscal year income when selected for a subcontract award, or DAI Global LLC may agree that registration using the D&B web form process is impractical in certain situations. Organizations may discuss these options with the DAI Global LLC representative.

What is CCR/SAM?
Central Contractor Registration (CCR)—which collected, validated, stored and disseminated data in support of agency acquisition and award missions—was consolidated with other federal systems into the System for Award Management (SAM). SAM is an official, free, U.S. government-operated website. There is NO charge to register or maintain your entity registration record in SAM.

When should I register in SAM?
While registration in SAM is not required for organizations receiving a grant under contract, subcontract or cooperative agreement from DAI Global LLC, DAI Global LLC requests that partners register in SAM if the organization meets the following criteria requiring executive compensation reporting in accordance with the FFATA regulations referenced above. SAM.gov registration allows an organization to directly report information and manage their organizational data instead of providing it to DAI Global LLC. Reporting on executive compensation for the five highest paid executives is required for a qualifying subaward if in your business or organization's preceding completed fiscal year, your business or organization (the legal entity to which the DUNS number belongs):

(1) received 80 percent or more of its annual gross revenues in U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements; **and**
(2) $25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements; **and**,

(3) The public have **does not** have access to information about the compensation of the executives in your business or organization (the legal entity to which the DUNS number it provided belongs) through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the US Internal Revenue Code of 1986.

If your organization meets the criteria to report executive compensation, the following sections of this document outline the benefits of and process for registration in SAM.gov. Registration may be initiated at https://www.sam.gov. There is NO fee to register for this site.

Why should I register in SAM?
DAI Global LLC recommends that partners register in SAM to facilitate their management of organizational data and certifications related to any U.S. federal funding, including required executive compensation reporting. Executive compensation reporting for the five highest paid executives is required in connection with the reporting of a qualifying subaward if:

a. In your business or organization's preceding completed fiscal year, your business or organization (the legal entity to which the DUNS number belongs) received (1) 80 percent or more of its annual gross revenues in U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements; and (2) $25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements; and,

b. The public have does not have access to information about the compensation of the executives in your business or organization (the legal entity to which the DUNS number it provided belongs) through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986.

What benefits do I receive from registering in SAM?
By registering in SAM, you gain the ability to bid on federal government contracts. Your registration does not guarantee your winning a government contract or increasing your level of business. Registration is simply a prerequisite before bidding on a contract. SAM also provides a central storage location for the registrant to supply its information, rather than with each federal agency or prime contractor separately. When information about your business changes, you only need to document the change in one place for every federal government agency to have the most up-to-date information.

How do I register in SAM?
Follow the step-by-step guidance for registering in SAM for assistance awards (under grants/cooperative agreements) at:
https://www.sam.gov/sam/transcript/Quick_Guide_for_Grants_Registrations.pdf

Follow the step-by-step guidance for contracts registrations at:
https://www.sam.gov/sam/transcript/Quick_Guide_for_Contract_Registrations.pdf

You must have a Data Universal Numbering System (DUNS) number in order to begin either registration process.

If you already have the necessary information on hand (see below), the online registration takes approximately one hour to complete, depending upon the size and complexity of your business or organization.

What data is needed to register in SAM?
SAM registrants are required to submit detailed information on their company in various categories. Additional, non-mandatory information is also requested. Categories of required and requested information include:

* General Information - Includes, but is not limited to, DUNS number, CAGE Code, company name, Federal Tax Identification Number (TIN), location, receipts, employee numbers, and web site address.

* Corporate Information - Includes, but is not limited to, organization or business type and SBA-defined socioeconomic characteristics.

* Goods and Services Information - Includes, but is not limited to, NAICS code, SIC code, Product Service (PSC) code, and Federal Supply Classification (FSC) code.

* Financial Information - Includes, but is not limited to, financial institution, American Banking Association (ABA) routing number, account number, remittance address, lock box number, automated clearing house (ACH) information, and credit card information.

* Point of Contact (POC) Information - Includes, but is not limited to, the primary and alternate points of contact and the electronic business, past performance, and government points of contact.
* Electronic Data Interchange (EDI) Information - Includes, but is not limited to, the EDI point of contact and his or her telephone, e-mail, and physical address.
(*Note: EDI Information is optional and may be provided only for businesses interested in conducting transactions through EDI.)

Attachment E: Self Certification for Exemption from DUNS Requirement

Legal Business Name:	
Physical Address:	
Physical City:	
Physical Foreign Province (if applicable):	
Physical Country:	
Signature of Certifier	
Full Name of Certifier (Last Name, First/Middle Names):	
Title of Certifier:	
Date of Certification (mm/dd/yyyy):	

The sub-contractor/vendor whose legal business name is provided herein, certifies that we are an organization exempt from obtaining a DUNS number, as the gross income received from all sources in the previous tax year is under USD $300,000.

*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.

Attachment F: Past Performance Form

Include projects that best illustrate your work experience relevant to this RFP, sorted by decreasing order of completion date.

Projects should have been undertaken in the past three years. Projects undertaken in the past six years may be taken into consideration at the discretion of the evaluation committee.

#	Project Title	Description of Activities	Location Province/ District	Client Name/Tel No	Cost in US$	Start-End Dates	Completed on schedule (Yes/No)	Completion Letter Received? (Yes/No)	Type of Agreement, Subcontract, Grant, PO (fixed price, cost reimbursable)
1									
2									
3									
4									
5									

Attachment G: Representations and Certifications of Compliance

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

7. Business Size and Classification(s) – The Bidder certifies that is has accurately and completely identified its business size and classification(s) herein in accordance with the definitions and requirements set forth in FAR Part 19, Small Business Programs.

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

9. Equal Opportunity – The Bidder 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.

10. Labor Laws – The Bidder certifies that it is in compliance with all labor laws..

11. Federal Acquisition Regulation (FAR) – The Bidder 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.

12. Employee Compliance – The Bidder warrants that it will require all employees, entities and individuals providing services in connection with the performance of an 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.

Attachment H: Proposal Checklist

Offeror: _____

Have you?

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

Does your proposal include the following?

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

☐ Separate Technical and Cost proposals individually sealed and labeled as Volume I and Volume II respectfully.

☐ Proposal of the Product or Service that meets the technical requirements as per Attachment A

☐ Response to each of the evaluation criteria

☐ Documents use to determine Responsibility

☐ Evidence of a DUNS Number OR Self Certification for Exemption from DUNS Requirement

☐ Past Performance *(use template in Attachment F)*

Attachment I: Technical Requirements

1.1 General

1.1.1 The TIP should offer on-premise and private cloud deployment options

The TIP should support both on-premise and private cloud-based deployment scenarios without a significant increase in architectural complexity or loss of functionality.

1.1.2 The TIP should support deployment on multiple hardware/software configurations (including VMware, Appliance and Standalone)

Provision of multiple deployment options enables the TIP to be integrated into a wider variety of environments.

1.1.3 The TIP should be vendor agnostic

The TIP must provide an open exchange for the consumption of threat intelligence from multiple sources. This should not be limited by product or vendor.

1.1.4 The TIP does not mine, capture, or store threat intelligence for use by a third-party

The TIP must not mine, capture or store any threat intelligence data for use outside of the end user organization. Threat intelligence must be owned solely by the end-user (organization) and must not be made available for use by a third-party entity.

1.1.5 The TIP must offer visualization capabilities to analyze and investigate threats

The threat data, which TIP is containing, should be visualized in a way that assists a user to better understand potential threats, collaborate with team members and then be able to take actions accordingly.

1.1.6 The TIP must offer a tasking, automation and workflow capability

The TIP should offer these mechanisms through direct interaction via a graphical user interface (GUI) or via third-party integration.

1.1.7 G008 – The TIP must have an integration with a threat intelligence provider. Demonstrate the list of integrations with 5+ threat intelligence providers.

1.2 Analyst Workbench and Threat Library

1.2.1 The TIP must have a Threat Library/database

TIP must be able to store data in an extensible library/database that allows for easy searching, manipulation, and enrichment of the data.

1.2.2 The TIP must offer user-defined scoring capabilities

The TIP must offer the organization the ability to define, customize and continually adjust scoring of Threat Indicators to meet their specific need. This must include the ability to weight scores by indicator type, attribute, source and adversary.

1.2.3 The TIP must continually update scores of stored threat intelligence

The TIP must be self-tuning. Specifically, it must be able to constantly evaluate and adjust indicator scores based on changes to environmental circumstances.

1.2.4 It must be possible to dynamically adjust scoring based upon external and internal threat data sources

It should be possible to influence scores and priorities using external sources of threat data such as a feed, an email or a report. In parallel users must have the option to utilize internal sources (such as SIEM events, active vulnerabilities, internal tickets) to influence scoring data.

1.2.5 The TIP should support the ingestion and export of threat data using multiple data types

The TIP should categorize threat intelligence by type. Filtering of Intelligence prior to export to the third party should be supported.

1.2.6 The TIP offers a flexible data model using custom objects

Administrators must be able to support all required data models and standards within a single searchable repository. The TIP data model should be extensible to meet these requirements using customizable objects.

1.2.7 The TIP must consolidate and expose all attributes from its threat intelligence feeds

Threat Intelligence sources generally provide additional context for indicators and adversaries in the form of attributes. It is important that these attributes are included and consolidated into the TIP and made available to the Analyst.

1.2.8 F009 – The TIP offers seamless data enrichment capabilities (e.g. VirusTotal, Domain Tools)

The TIP should support provisioning of additional enrichment capabilities. The TIP should support the addition of third-party data enrichment capabilities

The TIP should support capability to build custom tools into the product. Any custom enrichment tools must be installable via the GUI.

1.2.9 The TIP supports the de-duplication of threat intelligence from multiple input sources

A TIP should handle this process automatically as part of its aggregation process.

1.2.10 The TIP supports the normalization of threat intelligence sources into a single data model

The TIP must support the normalization and aggregation of this Intelligence into a single data model. This provides a single pane of glass for multiple Threat Intelligence sources.

1.2.11 The TIP should support the capability to introduce workflow when handling Threat Intelligence

Workflow enables a Security team to control the ingestion, evaluation, analysis and expiry of indicators. Should be the capability to create custom workflows.

1.2.12 The TIP should support user-defined data models

The TIP should provide a flexible data model that permits manipulation with types of threat data.

1.2.13 F016 – The TIP should be capable of supporting the association of multiple sources to a single indicator

A single view over multiple sources capability is a must.

1.2.14 The TIP should support timestamping of indicators for the provision of historical time-based analysis

Necessary for the historical analysis capabilities.

1.2.15 The TIP should support the categorization and analysis of adversaries

The TIP should assist with the categorization and reporting of indicators by adversary.

1.2.16 The TIP should support contextual information for all data objects

The TIP should associate contextual information such as TTP data to any object that is stored within the data model.

1.2.17 The TIP should support the provision of relationships between all objects within the data model

It must be possible to build relationships between all objects within the data model. This includes standard out-of-the-box objects as well as any that have been user-defined.

1.2.18 The TIP should support the upload of files such as TTP or Malware samples

The TIP should be able to associate this information to relevant indicators for further analysis as needed.

1.2.19 The TIP must offer a user-defined expiration capability

The TIP must offer a user definable expiration capability. This will enable to determine expiration of indicators.

1.3 Open Exchange (Interactions with third parties)

1.3.1 The TIP must have an Open Exchange

TIP must have an Open Exchange that allows other vendors, customers, or contractors to extend the functionality of the system through integrations.

1.3.2 The TIP must provide an API and SDK for the import and export of Threat Intelligence

The API and SDK provide a flexible interface for the provision of custom integrations.

1.3.3 The TIP should Query, Import, Export and Manage Threat Intelligence via the API

The API must be fully featured to enable seamless integrations.

1.3.4 The TIP must support ingestion of Threat Intelligence via multiple types (including CSV, PDF, ZIP, HTTP and Email formats)

The TIP must be able to ingest all this information to be effective.

1.3.5 The TIP should support the addition of custom Threat Intelligence feeds

This may include internal feeds or feeds that are provided by a managed service provider.

1.3.6 The TIP must support the filtering of output to minimize the export of unwanted Threat Intelligence

Filtering should be applied to a flexible data model to allow detailed views of Threat Intelligence to be created.

1.3.7 The TIP must support STIX 1.x

The XML-based STIX 1.x standard is utilized by a variety of feeds, sharing communities and CERTs. The TIP must support this standard to ensure compatibility with these types of sources.

1.3.8 The TIP must support STIX 2.x

The JSON-based STIX 2.x standard is increasingly in use by many feed providers, sharing communities and CERTs. The TIP should support this standard to ensure ongoing compatibility with sources of threat data.

1.3.9 The TIP must support STIX 1.x and STIX 2.x standards in parallel

The TIP must be able to consume data from STIX 1.x and STIX 2.x standards into the same data model. Where possible, the data should be interrelated automatically between the two standards. Users should be able to access, search and visualize data from both standards using a common user interface.

1.3.10 The TIP must support ingestion of multiple structured data formats

The TIP must be able to consume data from multiple structured data formats. All data should be accessible from a common interface and inter-related where possible. The TIP must support import and export of Threat Intelligence using TAXII

TAXII is a common format that is used by many CERTs and third-party Threat Intelligence providers.

1.3.11 The TIP should support bi-directional integration with common Intelligence Sharing Platforms

The TIP must support import and export of data from community driven intelligence sharing platforms. This includes both MISP and Soltra Edge. The TIP should be able to selectively import and export data.

1.3.12 The TIP must offer sharing options that are vendor agnostic

The TIP must offer sharing options that tie to an open and accessible sharing ecosystem. There should not be any requirement to leverage a proprietary vendor-based technology.

1.3.13 The TIP must support bidirectional integration with the SIEM

Bi-directional integration with a SIEM should enable:

- SIEM can filter alerts/events against active Threat Intelligence. Thus, enabling prioritization of potential threats.
- SIEM can ingest Threat Intelligence for use in its own correlation capability.
- SIEM can add and modify indicators within the TIP. E.g. an indicator that is identified as a false positive can be marked as such within the.

1.3.14 The TIP must support bi-directional integration with a standard ticketing system or Incident Response ticketing system

Bi-directional integration with a ticketing system should enable:,

- Auto-population of tickets with relevant Threat Intelligence information.
- Ability to search for related indicators from within the ticketing solution.
- The ticketing system may add and modify indicators within the TIP. E.g. Add an indicator that has been identified as part of a forensic analysis that is new and not present in the TIP.
- Syncing of tasks and incidents between the TIP and the ticketing/IR tool.

1.3.15 The TIP must support the ingestion of third-party event feeds (e.g. Dynamic Analysis/Malware, News Alerts and Social Media)

Ingestion of third-party event feeds provides additional enrichment for indicators. This additional context may then be used by analysts to make more informed decisions about a potential threat.

1.3.16 The TIP must support the addition of data enrichment sources

The TIP must support the addition of data enrichment sources that are not available out of the box.

1.3.17 The TIP should support integration with third party Vulnerability Assessment tools

The TIP should offer the ability to correlate threat data with vulnerability data from current or defined scans. It should be possible to build data enrichment functions to look up specific vulnerability information from within the TIP on demand.

1.3.18 The TIP must integrate with Orchestration Tools

Third-party orchestration tools must be able to leverage the TIP as part of a workflow or playbook. The TIP should offer bi-directional integration capabilities where possible.

1.3.19 Methods of integration should be clearly documented to allow for third-party development

All methods of interaction with the TIP must be clearly documented with examples, including APIs and SDKs.

1.3.20 The TIP must be able to ingest MITRE ATT&CK data

The TIP must be able to capture data from MITRE ATT&CK. All categories of ATT&CK data must be available and independently selectable. This includes Tactics, Techniques, Groups/Adversaries, Mitigations, Tools and Malware data.

1.4 Reporting, Analysis & Search

1.4.1 The TIP must support the generation of reports

Reporting enables management level visibility of Threat Intelligence.

1.4.2 The TIP should support object specific reporting and analysis.

The TIP should provide detailed reporting for objects (e.g. adversaries, indicators and attack techniques).

1.4.3 The TIP must support keyword search

The TIP must support simple keyword search. This should be accessible from within the GUI but also via integration points such as API or SDK.

1.4.4 The TIP must support advanced searching using filters

The TIP must support filters to define and limit searches. Filters should include,

- Date/Time
- Relationship association
- Attribute matching
- Type filtering
- Score filtering

1.4.5 Searches should support multiple operators

The TIP must enable users to define searches using comparative operators (e.g. contains, equals, does not equal) and arithmetic operators (e.g. greater or less than, equals, does not equal).

1.4.6 Searches should support multiple criteria sets

Searching must support the creation of specific criteria sets that incorporates a combination of search terms and filters. It should be possible to create multiple criteria sets to search for different results. It must be possible use Boolean operators (AND, OR) between criteria sets to focus searches and narrow down result sets.

1.4.7 It must be possible to save searches

The TIP must be able to save searches for use at a later stage. These searches should be available by a dedicated and authenticated web URL.

1.4.8 The TIP must offer drill-down capabilities for search results

A user must be able to drill-down in into the detailed data that is associated with each search result. Drill-down must occur without losing access to the original set of search results.

1.4.9 Third parties must have access to search features via UI and API

All search features must be accessible from within the UI. Third parties must be able to access the same features via the API to assist with automation and integration tasks.

1.4.10 The TIP must offer user defined dashboards

Each dashboard must be customizable and offer a range of different visualization options. Users must be able to define the location, size and content for each dashboard independently. It should be possible to drill-down into each dashboard widget.

1.4.11 It must be possible to create multiple dashboards and restrict access accordingly

Users must be able to define and create multiple dashboards within the TIP. Users must be able to limit access to specific dashboards using permissions.

1.4.12 It must be possible to share dashboards with other users

Users must be able to share a set of dashboards with other users that have access to the TIP.

1.5 Visual Investigation

1.5.1 The TIP must offer a visual interface for performing investigations using threat intelligence

It is important to provide a visual investigations capability that enables users to represent this data in a format that may be easier understood and to allow investigations to take place easier.

1.5.2 A visual investigation must offer tools for multiple teams to collaborate in real-time

The TIP must offer tools for teams to collaborate in real-time when using threat intelligence data. This must include a visual investigations capability and a tasking facility.

1.5.3 The visual investigation must offer independent workspaces for users to research threats prior to contributing to an investigation

It is important to provide users with individual workspaces where this necessary activity may take place, whilst offering capabilities to add important data points to the investigation itself when required.

1.5.4 Visual investigations must offer timeline capabilities

Timelines are an essential part of any investigation as they offer an insight into the time frame of a potential breach or other relevant data. The TIP's visual analytics capability must represent this data on screen to provide better context for investigations.

1.5.5 Visual investigations must provision access to third-party enrichments from within its interface

The TIP should offer access to enrichment capabilities from within its visual investigations interface.

1.5.6 Visual investigations must link to the underlying data model

The visual investigations interface must link to the underlying data model and synchronize data between the two.

1.5.7 Users must be able to assign tasks from within a visual investigation

Tasking must be available to assign actions to others. This should be accessible from within the TIP and the visual investigation.

1.6 Data Exchange and Sharing

1.6.1 The TIP must have the ability to be deployed with multiple instances that allow for the sharing or exchange of data between them.

The TIP should provide the ability to exchange information from one instance to another.

1.6.2 The TIP must support open standards of data exchange and not force a proprietary ecosystem.

The TIP must support an open standard to allow open-source technology to participate in exchange.