CADMUS

REQUEST FOR PROPOSAL (RFP)

Digital Traceability

TO: Potential Bidders

FROM: Darlene Irby, Project Director
The Cadmus Group
Digital Forward
Contract No. 7200AA23C00131

ISSUANCE DATE:	October 7, 2024
DEADLINE FOR RECEIPT OF QUESTIONS:	October 11, 2024, 5:00 PM EDT
SUBMISSION DATE:	November 8, 2024, 5:00 PM EDT

USAID Digital Forward, in conjunction with the German Federal Ministry for Economic Cooperation and Development (Bundesministerium fur wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)), is seeking technical and price proposals from eligible firms capable of conducting a study that aims to examine the use of digital tools to facilitate smallholder farmers in low- and middle-income countries' ability to contribute field and production data for traceability purposes, including those needed for certification and/or regulatory compliance (such as the European Union Regulation on Deforestation Free Products and others).

Cadmus, as the prime implementor of the U.S. Agency for International Development (USAID)-funded Digital Forward project intends to award a firm-fixed-price type contract for this activity. The agreement between the implementer and BMZ will be determined at time of selection. The start date of this activity is on/about January 6, 2024. The total estimated value of this RFP is up to USD $210,00.00 ($100,00.00 to be funded by USAID through Cadmus, and €100,000.00 from BMZ).

This RFP is open to qualified companies with experience in what is required in the scope of work under Section C.

All potential offerors are also informed that the contractor that is awarded a contract pursuant to this RFP will not be eligible to participate in any subsequent RFPs that involves evaluation of work done under this RFP, or any other activity that may result in conflict of interest because of the work performed under this RFP.

Technical and price proposal requirements, as well as proposal evaluation criteria, are outlined **in Sections L and M, respectively**. Cadmus and BMZ, each, intend to make a subcontract award to the responsible Offeror whose proposal represents the best value to the U.S. government and BMZ.

Proposals are due in electronic copy only, in MS Word, MS Excel, and/or PDF formats, by November 8, 2024 at 5:00 PM EDT. Tables or charts in MS Excel format should be labeled appropriately. The email must not exceed 5MB in size. Technical and price proposals need to be submitted in separate electronic files and emailed to Arthur.muchajer@cadmusgroup.com.

Proposals should include filled out and signed documentation in **Section J**. All offerors should also review information included in **Section H and I**.

Questions regarding this RFP are due in electronic copy by October 11, 2024 at 5:00 PM EST time. They must be emailed (no phone questions will be accepted) to Arthur.muchajer@cadmusgroup.com. Potential bidders who do not submit questions should send an email with their contact information if they wish to receive copies of answers. All questions and responses will be circulated to all offerors who ask questions and to those who register.

This RFP, including this cover letter, in no way obligates Cadmus or GMZ to award a contract nor does it commit Cadmus or GMZ to pay for any costs incurred in the preparation and submission of a proposal in response hereto. Furthermore, Cadmus reserves the right to reject any and all offers, if such action is considered to be in the best interest of USAID, while GMZ can reject all offers as well, is such action is considered to be in their best interest.

All BMZ terms and conditions will be provided to the offeror being chosen by the evaluation committee to implement the scope of work.

Sincerely,

DocuSigned by:
Darlene Irby
4F68315E6062448...

Darlene Irby, Project Director
The Cadmus Group
Digital Forward

PART I – THE SCHEDULE

B. SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Purpose

The purpose of this activity is to provide USAID, BMZ, and their partners with a better understanding of the current state of digital technologies that are being used to facilitate traceability and compliance in the agriculture sector, with a particular focus on smallholder farmers.

B.2 Contract Type

Cadmus, as the prime implementor of the U.S. Agency for International Development (USAID)-funded Digital Forward intends to award a firm-fixed-price type contract for this activity. Cadmus reserves the right to select a different contract type if necessary.

B.3 Contract Price

The price of each contract will not exceed $100,000.00 (with Cadmus) and €100,000.00 (with BMZ) for the performance of the work required hereunder and delivery of the deliverables. Under no circumstances will the subcontractor be paid any amount in excess of these amounts without formal contract modification signed by the respective parties.

B.4 Payment

The Payment Schedule for the contract is to be proposed by the offeror based on the milestones/deliverables listed below.

Milestone/Deliverable	Payment Amount	Payer	Due Date
Rapid Analysis (desk research and key stakeholder interviews) and Madagascar Deep Dive	$		March 31, 2025
Draft Report	$		April 30, 2025
Stakeholder feedback sessions (and accompanying slide deck)	$		May 30, 2025
Final Report including Madagascar deep dive as a section and also as a standalone report and Policy Dialogue (and accompanying slide deck)	$		June 30, 2025
TOTAL	$		

Payment of a milestone/deliverable will be made for an accepted and approved milestone/deliverable by Cadmus, BMZ and USAID.

B.5 Indirect Costs

Offerors should include their rates in the table below that are in line with their negotiated government rates (if applicable) or those in line with their audited rates. Those Offerors that do not have negotiated rates can propose them in the table below.

Reimbursement for indirect costs will be at final negotiated rates, but not in excess of the following ceiling rates:

Description	**Rate**	**Base of Application**
Fringe		
Overhead		
G&A		

Cadmus will not be obligated to pay any additional amount should the final indirect cost rates exceed the negotiated ceiling rates. If the final indirect cost rates are less than the negotiated ceiling rates, the negotiated rates will be reduced to conform with the lower rates.

This understanding must not change any monetary ceiling, obligation, or specific cost allowance or disallowance. Any changes in classifying or allocating indirect costs require the prior written approval of Cadmus's Contracts Administrator.

[End of Section B]

C. DESCRIPTION/SPECIFICATIONS/STATE OF WORK

Digital Forward Background

Launched in February 2024, the Digital Forward Mechanism aims to bolster USAID and implementing partner efforts to design, support and implement digital technology programs; accelerate open, inclusive and secure digital ecosystems; and disseminate knowledge within USAID and the development community on the digital technology's best practices, successes, and lessons learned from programs. The Activity will implement work that advance two mutually reinforcing objectives:

- Objective 1: Support USAID with Digital Development-focused technical assistance, research, training, strategic thinking, digital-sector partnerships, and behavior change that will equip USAID programming for the digital age, and
- Objective 2: Support the growth of open, inclusive, and secure digital ecosystems in partner countries through work with USAID.

Digital Forward is managed through the Innovation, Technology, & Research Hub's Technology Division (ITR/T) within the Bureau for Development, Democracy, and Innovation (DDI).

Activity Background

In recent years, the combination of increased consumer demand to better understand the provenance of agricultural products they purchase, increased uptake of supply chain and environmental certifications, and new regulatory requirements, have increased the need for tools that can be used to accurately verify supply chain traceability in the agriculture sector. A range of digital technologies have been deployed by different actors to facilitate the collection, management and verification of requisite data. Yet, smallholder farmers often lack access to and/or a sufficient understanding of how to use the underlying digital technologies required for these purposes, particularly in low- and middle-income countries (LMICs).

While there have been a number of efforts made to make these tools more accessible to smallholder farmers, including using intermediaries with digital tools to facilitate access, there has not yet been a comprehensive study analyzing the current state of digital traceability through the lens of smallholder farmers in these markets.

The study aims to examine the use of digital tools to facilitate smallholder farmers in low- and middle-income countries' ability to contribute field and production data for traceability purposes, including those needed for certification and/or regulatory compliance (such as the European Union Regulation on Deforestation Free Products and others). It should be based on desk research and key informant interviews and/or focus groups with agribusinesses, technology companies, government agencies, producer organizations, and other relevant stakeholders.

The study should examine underlying factors impacting smallholder readiness to use and benefit from digital traceability and other relevant monitoring, reporting, and verification (MRV) tools, the business case for their adoption by different value chain actors (such as farmers, buyers, distributors, brands), promising examples of such tools and associated business models, barriers to smallholder uptake, the role of different stakeholders in enabling smallholder uptake (such as cooperatives, exporters, government agencies, and others), dependent systems that may be required to facilitate their successful deployment (such as land registries and ID systems), and alternative models for verification that help to address such barriers. It may also include a focus on specifications and requirements of any relevant tools. Particular attention should be paid to inclusive access to and usage of such tools (including, but not limited to, gender, indigeneity, social and economic status, and others) in relation to the above. The study should also explore methods for empowering smallholders to have greater control of and financial benefit from data that is collected about their farms and practices rather than being primarily extractive, as well as approaches to safeguarding farmer and farm data, and mitigating the perceived risk or any hesitancy that farmers and other value chain actors may have about sharing this data. This may include an examination of approaches for attaching attributes to value chain data (e.g. that produce comes from a farm that is deforestation free, without sharing specific farmer or farm data along the value chain). It should also explore the role of digital public infrastructure and open data as enablers of traceability and compliance in the agriculture sector, including potential prerequisites, opportunities, barriers, and ways to potentially address those barriers.

It will be important for the study to examine existing efforts and research to strengthen traceability for smallholders, including, but not limited to, the work being done by the Digital Integration of Agricultural Supply Chains Alliance (DIASCA), INATrace, and the Forest Data Partnership. Where relevant, it should also build off of previous work related to data governance, such as the Farmer-Centric Data Governance: Towards A New Paradigm report, the Data Sovereignty in Agricultural Value Chains report, and the Toolkit for Ethical Data Governance in Agriculture.

It is expected that this study will broadly cover the state of digital traceability for smallholder farmers in LMICs, although bidders are not expected to comprehensively examine every LMIC or agricultural value chain. Bidders should explain how they would make the study broadly representative while also taking into account differences that may exist between countries or regions.

Additionally, bidders are required to conduct a country-specific deep dive for Madagascar. The deep dive should focus on the use of digital tools to facilitate smallholder farmers in Madagascar's ability to contribute field and production data for traceability purposes, including those needed for certification and/or regulatory compliance, in line with the overall study. It should focus specifically on the vanilla and spices value chains with a geographical focus in the Southeast (Vatovavy, Fitovinany and Atsimo Atsinanana) and North (Sava). As with the global study, it should include both desk research and key informant interviews and/or focus group discussions. Bidders should mention explicitly what modalities they will use and the minimum number of people they will interview and/or include in focus group discussions. Exclusive to this portion of the activity, bidders will be required to demonstrate that at least 65% of the level of effort associated with the deep dive comes from individuals or firms local to Madagascar.

All of the focus areas highlighted above for the global study should be applied to the Madagascar deep dive. In addition, it should provide specific recommendations on options for digital traceability tools that can be used in these value chains within the context of these geographic regions. The options provided may be off-the-shelf or require customization, and should include a rough estimate of the cost of deployment as well as suggestions for how each option could be deployed to Madagascar without ongoing donor funding.

Activity Objectives

The objective of this assignment is to provide USAID, BMZ, and their partners with a better understanding of the current state of digital technologies that are being used to facilitate traceability and compliance in the agriculture sector, with a particular focus on smallholder farmers. It aims to provide tangible and actionable recommendations for policymakers, donors, agribusinesses, technology companies, and organizations that support smallholders to be better equipped to benefit from digital traceability and compliance tools.

Activity Tasks

It is envisioned that this assignment will entail the following tasks, although bidders are welcome to propose additional tasks or modifications to the proposed tasks if they feel that such changes will be more effective at achieving the overall objectives of this assignment.

1. TASK 1: Rapid Analysis and Report

The rapid analysis will seek to identify the current state and likely trends in digital traceability as they relate to smallholder farmers in LMICs broadly and Madagascar specifically. In particular, it should include:

- Desk research of existing literature on digital traceability and related sectors
- Review of existing policy and regulatory efforts (both enacted and proposed) from around the world related to traceability and compliance
- Key informant interviews and/or focus group discussions with industry experts in this space, as well as individuals who can represent the perspective of agri-food system actors, such as farmer organizations, agribusinesses, civil society organizations, technology companies, regulatory bodies, and others. These should be done for both the overall study and the Madagascar deep dive. Bidders are required to include the minimum number of people they will speak with and the modalities they will use in their proposal. The list of proposed informants will be developed by the selected firm and are not required as part of the proposal, although illustrative informants are welcome.

The findings from the rapid analysis will be synthesized into a report that includes, at a minimum, the following content:

- An overview of the current state of digital traceability in agri-food systems in LMICs
- A summary of the underlying factors impacting smallholder readiness to use and benefit from digital traceability tools, the business case for their adoption by different value chain actors, promising examples of such tools and associated business models, barriers to smallholder uptake, the role of different stakeholders in enabling smallholder uptake, and alternative models for verification that help to address such barriers.

- A summary of promising methods for empowering smallholders to have greater control of and financial benefit from data that is collected about their farms and practices, as well as approaches to safeguarding farmer and farm data.
- An examination of the role of digital public infrastructure and open data as enablers of traceability and compliance in the agriculture sector, including potential prerequisites, opportunities, and barriers.
- A deep dive case study for Madagascar including the four points above specific to the value chains and geographic regions outlined in the activity overview, along with country specific recommendations.
- A list of tangible and actionable recommendations for policymakers, donors, agribusinesses, technology companies, and organizations that support smallholders to be better equipped to benefit from digital traceability tools.
- A list of organizations and companies who are working on issues related to responsible and

inclusive digital traceability globally, including descriptions of their work, geographic focus, and actionable opportunities for future engagement, where relevant.

2. TASK 2: Stakeholder feedback sessions

Once a draft report is developed, the key findings and recommendations will be presented to key stakeholders, including key informants interviewed during Task 1, select USG staff, BMZ and other invited parties, as proposed by the selected firm, USAID and BMZ. The purpose of these sessions will be to solicit feedback from participants on the report's findings and recommendations to strengthen the final product. It is anticipated that two sessions will be held to enable individuals from all time zones to participate, with both conducted virtually. An additional and separate session should also be held with select local stakeholders in Madagascar, including staff from USAID/Madagascar, BMZ and its local partners, and other invited parties as proposed by the selected firm, USAID, and BMZ.

3. TASK 3: Public dialogue

The final report's key findings and recommendations will be presented during a virtual event(s) (either standalone or as part of a relevant, pre-existing event) aimed at both promoting awareness and facilitating stakeholder dialogue in an inclusive manner that includes stakeholders representing the technology sector, relevant government agencies and development organizations, the agriculture sector (both agribusinesses and farmer organizations), and civil society. Bidders are encouraged to propose a high-level structure for the event(s) and approach to increasing the likelihood that the public dialogue results in potential action.

Activity Deliverables

The below is an illustrative general timeline for this work. If firms have a different proposed timeline they recommend they are welcome to propose it.

DELIVERABLES	TIMEFRAME
Rapid Analysis (desk research and key stakeholder interviews)	January-March 2025

Madagascar Deep Dive	February-March 2025
Draft Report	April 2025
Stakeholder feedback sessions (and accompanying slide deck)	May 2025
Final Report including Madagascar deep dive as a section and also as a standalone report	June 2025
Policy dialogue (and accompanying slide deck)	June 2025

Note: All deliverables are subject to review and acceptance by Digital Forward.

Travel

There is no international travel envisioned for this activity, however, in country travel may be proposed, if relevant, for the deep dive study in Madagascar.

Place of Performance

While the focus of this study is both global and Madagascar, the place of performance for this activity will be remote. The inclusion of local, in country expertise is required for the deep dive study in Madagascar.

Activity Period of Performance

The period of performance for this activity is anticipated to be o/a January 6, 2025 – o/a July 11, 2025

Reporting

The selected bidder will receive two separate contracts for this work, one through Digital Forward on behalf of USAID and the other directly with BMZ. Both contracts will include the same milestones. As such, the selected bidder will work closely with Digital Forward, USAID, and BMZ.

[End of Section C]

D. PACKAGING AND MARKING

Section D and its contents here within are only applicable to the USAID portion of funding.

Branding and Marking will be compliant with the Digital Forward's approved Branding and Marking Plan. Cadmus will provide specific requirements for branding and marking upon issuing an award. Information about USAID branding and marking can be found at ADS Chapter 320 | Document | U.S. Agency for International Development (usaid.gov).

[End of Section D]

E. INSPECTION AND ACCEPTANCE

Section E and its contents here within are only applicable to the USAID portion of funding.

E.1 Notice Listing Contract Clauses Incorporated by Reference

In accordance with FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract, the following contract clauses are hereby incorporated by reference, with the same force and effect as if they were given in full text. See https://www.acquisition.gov/browse/index/far / for electronic access to the full text of a clause.

Number	Title	Date
52.246-4	Inspection of Services-Fixed-Price	August 1996

E.2 Inspection and Acceptance

Inspection and acceptance of services, reports and other required deliverables or outputs shall take place at principal place of performance or at any other location where the services are performed and reports and deliverables or outputs are produced or submitted. Unless otherwise stated, the designated Cadmus Technical Representative will inspect and accept all services, reports and required deliverables or outputs. USAID may also play a significant role in inspecting and accepting all services, reports and required deliverables or outputs.

[End of Section E]

F. DELIVERIES OR PERFORMANCE

F.1 Place of Performance

While the focus of this study is both global and Madagascar, the place of performance for this activity will be remote. The inclusion of local, in country expertise is required for the deep dive study in Madagascar.

F.2 Period of Performance

The period of performance anticipated herein will be six (6) months from the date of award signature.

Start Date: on/about January 6, 2025

End Date: on/about July 11, 2025

F.3 Performance Standards

Contractor agrees to provide the services required hereunder in accordance with the requirements set forth in this Agreement. Contractor undertakes to perform the services hereunder in accordance with the highest standards of professional and ethical competence and integrity in Contractor's industry, having due regard for the nature and purposes of The Cadmus Group and to ensure that employees assigned to perform any services under this Agreement will conduct themselves in a manner consistent therewith. The services will be rendered by the Contractor in 1) an efficient, safe, courteous, and businesslike manner; 2) in accordance with any specific instructions issued from time to time by The Cadmus Group, Contractor shall provide the services of qualified personnel through all stages of this Agreement. Contractor shall promptly replace any member of the Contractor's project team that The Cadmus Group considers unfit or otherwise unsatisfactory.

F.4 Key Personnel and Other Staffing

A. Key personnel are those Subcontractor personnel considered to be essential to the performance of the Work, and designated by name as key personnel. The key personnel required for this activity are:

   - Assessment Lead
   - In-Country Madagascar Lead

B. Prior to replacing key personnel, the Subcontractor shall demonstrate to the satisfaction of the Cadmus Technical Representative that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the personnel being replaced.

C. All requests for replacement must provide a detailed explanation of the circumstances necessitating the proposed replacement, a complete resume for the person proposed as the replacement, and any additional information reasonably requested by Cadmus to approve or disapprove the proposed replacement.

D. Any changes to Subcontractor key personnel may also require the acceptance and approval of Cadmus's Client.

F.4 Reports and Deliverables

All reports and other deliverables must be in the English language. All reports and other deliverables must be submitted to the Cadmus Project Manager listed in Section G.2.

Reporting:

- Subcontractor shall furnish monthly status **reports**, as directed, if required, by the Cadmus Project Manager.
- Cadmus may have an obligation to report certain direct labor hours utilized in the performance of its work. Therefore, Subcontractor may be required to report direct labor hours for professional personnel performing technical work. These hours shall be reported by category, or as directed by Cadmus Project Manager. Indirect administrative support hours are not considered direct labor for purposes of this reporting, even if they are charged as direct under Subcontractor's accounting practices. These support hours shall be classified as "other" for reporting purposes. Direct labor hours furnished by consultants and lower-tier Subcontractors, if any, shall also be reported.

Deliverables:

- All deliverables shall be forwarded to the Cadmus Project Manager by Subcontractor at the time of submittal. Deliverables submitted under this Agreement shall cite the Subcontractor name, contract number, Agreement number and shall identify Cadmus as the Prime Contractor and Client as the sponsoring agency. Additional reporting requirements may be identified by the Cadmus Project Manager. The Cadmus Project Manager will approve all deliverables submitted under this subcontract.
- Deliverables Table

MILESTONES/DELIVERABLES*	TIMEFRAME
Rapid Analysis (desk research and key stakeholder interviews)	January-March 2025
Madagascar Deep Dive	February-March 2025
Draft Report	April 2025
Stakeholder feedback sessions (and accompanying slide deck)	May 2025
Final Report including Madagascar deep dive as a section and also as a standalone report	June 2025
Policy dialogue (and accompanying slide deck)	June 2025

*Descriptions of the deliverables can be found under Section C.

[End of Section F]

G. CONTRACT ADMINISTRATION DATA

Section G and its contents here within are only applicable to the USAID portion of funding.

G.1 Invoicing and Payment

A. A separate invoice must be prepared for each Agreement. To be eligible for payment, all invoices must include the following information:

(i) Subcontract number
(ii) Dates (to and from) covered in invoice
(iii) Description of work performed
(iv) Itemized expenses and receipts for all travel expenses and ODCs expenses that are authorized
(v) Payment remittance information
(vi) Cumulative and current totals invoiced for the Agreement
(vii) Cadmus Project Manager
(viii) If required by the Cadmus Project Manager, reference codes for labor and authorized expenses
(ix) Upon completion of Work, Subcontractor must submit a final invoice, marked “Final Invoice” for all Work performed. The final invoice, in addition to billing for all final period costs shall summarize all previous invoices and payments made for the project and indicate the total final project amount.

Under no circumstances shall alcohol, entertainment, or other personal expenses be billed to Cadmus or the Clients.

Invoices shall include the following certification: " *I HEREBY CERTIFY THIS INVOICE CORRECTLY REFLECTS CHARGES FOR SERVICES PROVIDED DURING THE STATED PERIOD, AND TO FURTHER CERTIFY THAT ALL PERSONNEL BEING BILLED MEET OR EXCEED ANY LABOR CATEGORY QUALIFICATIONS INCLUDED AS PART OF THIS AGREEMENT".*

B. Invoices shall reference the name and signature of a certifying officer of Subcontractor. INVOICES SHALL BE SENT ELECTRONICALLY to **idd.accountspayable@cadmusgroup.com** and the Cadmus Project Manager. Only if Subcontractor is unable to provide electronic invoices may Subcontractor submit invoices by fax to (617) 673-7330 or by mail to the attention of:

Accounts Payable
The Cadmus Group LLC
800 N. Glebe Road, Suite 500
Arlington, VA 22203

C. Invoices for completed work may be submitted in accordance with Section G.1 of this Agreement. The period covered by invoices or requests for Subcontractor payments shall be the same as the period for monthly progress reports, if any, required. Where cumulative amounts on the monthly progress report differ from the aggregate amounts claimed in the invoice(s) or request(s) for payments covering the same period, Subcontractor shall provide a reconciliation of the difference as part of the payment request.

D. Any holdback or disallowance of costs that the Client may impose with respect to all or part of Subcontractor's invoice shall be withheld from Subcontractor. In the event that the Client (a) disallows any costs or fee for which Cadmus has reimbursed Subcontractor hereunder or (b) reduces the costs or fee payable to Cadmus under the Contract as a result of (i) any defective cost or pricing data submitted by Subcontractor or (ii) any adjustment based upon Subcontractor work performance or personnel issues, Subcontractor shall promptly pay to Cadmus the amount of any such disallowance or reduction. Cadmus may withhold such amounts from any other sums then due and payable to Subcontractor, if Subcontractor fails to make payment of such amounts in a timely manner.

E. Subcontractor may prepare its invoice or request for payment on the prescribed Government forms. Standard Form Number 1034, Public Voucher for Purchases and Services other than Personal, may be used to show the amount claimed for reimbursement. Standard Form 1035, Public Voucher for Purchases and Services other than Personal--Continuation Sheet, may be used to furnish the necessary supporting detail or additional information required. Subcontractor may submit self-designed forms which contain the information required by this Agreement. A sample copy of an acceptable invoice format may be provided upon request.

F. Unless otherwise specified, all charges shall be invoiced no later than 30 days after the end of the Period of Performance.

G. Subcontractor's invoices will be considered to be in proper form only if each meets all of the requirements set forth in this Agreement. Subcontractor will be paid ten (10) days after Cadmus receives payment from the Client, not to exceed 75 days after receiving an acceptable invoice in the proper form.

H. Payment by Cadmus will be made in ***US Dollars.*** Cadmus will pay the subcontractor within thirty (30) calendar days after receipt of a proper invoice following the instructions of Section G.1 and acceptance and approval of deliverables.

G.2 Technical Direction

In regard to technical matters related to this Agreement, the parties hereby appoint the below listed persons as their Technical Representative, which may also be referred to as Cadmus Project Manager:

For Cadmus		**For Subcontractor**	
Name	Taunya Atwood	**Name**	
Address	800 N. Glebe Road Suite 500 Arlington, VA 22203	**Address**	
Phone	+1 (703) 516-7857	**Phone**	

Email	Taunya.atwood@cadmusgroup.com	**Email**	

G.3 Subcontract Administration

In regard to administrative and contractual matters related to this Agreement, the parties hereby appoint the below listed person, or their duly authorized designees for subcontract administration, as the only persons empowered to make commitments on behalf of their respective organization to effect changes to any portions of this Agreement.

For Cadmus		**For Subcontractor**	
Name	Arthur Muchajer	**Name**	**Click or tap here to enter text.**
Address	800 N. Glebe Road Suite 500 Arlington, VA 22203	**Address**	**Click or tap here to enter text.** **Click or tap here to enter text.** **Click or tap here to enter text.** **Click or tap here to enter text.** **Click or tap here to enter text.**
Phone	+1 (703) 247-6053	**Phone**	**Click or tap here to enter text.**
Email	Arthur.muchajer@cadmusgroup.com	**Email**	**Click or tap here to enter text.**

G.7 Subcontractor's Payment Address

To be incorporated upon award.

[End of Section G]

H. SPECIAL CONTRACT REQUIREMENTS

Section H and its contents here within are only applicable to the USAID portion of funding.

H.1 Disclosure

During the term of this Agreement, Cadmus and Subcontractor may be required to make available to each other certain information which the Parties may consider Proprietary and/or Confidential. Such information shall be disclosed subject to and in accordance with the terms set forth in the Non-Disclosure Agreement related to this Program, which is hereby incorporated by reference, except the term of the Non-Disclosure Agreement is hereby changed to match the term of this Agreement.

H.2 Data Security

A. In addition to the confidentiality terms contained above, Subcontractor shall exercise all due care with respect to securing data provided to Subcontractor, particularly sensitive data such as Personal Information. Personal Information shall mean any data or information, or portion thereof, that is not publicly available and could be used, alone or in conjunction with any other information, to identify or authenticate a specific person. Examples of Personal Information include but are not limited to a) billing account number; (b) natural person's name, street address, telephone number, e-mail address, photograph, social security number or tax identification number, driver's license number, passport number, credit card number, bank information, health information, device identifiers, IP addresses, biometric identifiers or any other piece of information that alone or in combination with other information allows the identification of or contact with a natural person; and (c) information that is associated, directly or indirectly (by, for example, records linked via unique keys), to any of the foregoing, such as historical sales, usage, billing and payment information. Prior to receipt of Personal Information in performance of Work under this Agreement, Subcontractor must complete a Cadmus Information Security Questionnaire.

   Subcontractor must implement administrative, physical, and technical controls to ensure that the collection, handling, delivery, processing, transmission, and storage of such sensitive data conforms to industry best practices, including, but not limited to NIST 800-53 or ISO 27001, to ensure its confidentiality, integrity, and availability. Subcontractor shall further treat all sensitive data in accordance with applicable federal, state, and local laws, including privacy laws and laws regarding unauthorized access, confidentiality and security. To the extent Subcontractor collects or receives Personal Information from a natural person, Cadmus, or Cadmus' Client, Subcontractor shall comply with applicable state privacy laws; to include the California Consumer Privacy Act (CCPA), which specifically prohibits the retention, use or disclosure of Personal Information of California residents for any purpose other than the specific purpose of performing the services specified in this Agreement.

   To the extent Subcontractor receives personal data of any citizen of the European Union (EU), that data will be treated in conformance with the requirements of the EU General Data Protection Regulation.

B. Security Incidents. Subcontractor will notify Cadmus in writing within 24 hours of any actual, threatened or reasonably suspected unauthorized access, use or disclosure of data

provided to Subcontractor. Subcontractor will retain all relevant records, logs, files, and data relevant to the incident for forensic analysis. Subcontractor will cooperate with Cadmus and the Client in investigating the incident and provide information necessary for notice to be provided to individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as may be required by law.

H.3 Intellectual Property

During the performance of this Agreement, the following provision shall apply with respect to all materials and work products developed and/or delivered by Subcontractor:

A. If FAR 52.227-11 or FAR 52.227-12 is applicable to the Prime Contract, Cadmus shall flow such clause down to Subcontractor, and Subcontractor shall retain rights in Subject Inventions as defined in such clause and shall be bound by all reporting and other obligations therein. In addition, Cadmus's Client shall retain the rights granted to the Government under such clause. Except with respect to any rights in Subject Inventions retained by the Subcontractor and/or as permitted under paragraph B below, Subcontractor agrees that all materials and work products that it develops under this Agreement, including software and documentation, shall be considered "Works for Hire." All Works for Hire shall be owned exclusively by Cadmus or Cadmus's Client, and Subcontractor will have no property or other proprietary rights in them. Works for Hire shall be turned over to Cadmus promptly upon Cadmus's request and upon termination or expiration of this Agreement. Subcontractor agrees to assign to Cadmus all right, title, and interest in and to all Works for Hire created by Subcontractor hereunder. Additionally, Subcontractor shall take all acts and execute all documents reasonably necessary in order to affect such assignment, at Cadmus's expense.

B. If Defense Federal Acquisition Regulations Supplement ("DFARS") clause 252.227-7013 is applicable to this Agreement, any technical data (as defined in that clause) provided by Subcontractor under this Agreement will be governed by that clause. If DFARS clause 252.227-7014 is applicable to this Agreement, any noncommercial computer software and noncommercial computer software documentation (as each term is defined in such clause) will be governed by that clause. No clause in this Agreement will be interpreted as enlarging or diminishing the Client's, Cadmus's, or any other subcontractor's or supplier's rights in Subcontractor's technical data and/or noncommercial computer software and noncommercial computer software documentation, as the case may be.

C. Subcontractor's pre-existing tools, techniques and other intellectual property that Subcontractor uses in providing services under this Agreement ("pre-existing work") shall not be considered "Works for Hire" under this clause and shall be owned exclusively by Subcontractor or its licensor, as the case may be, provided that Subcontractor clearly marks all such pre-existing works as required by the applicable FAR and/or DFARS clauses and notifies Cadmus in writing of all such pre-existing works prior to execution of this Agreement, or if such cannot be identified at such time, then promptly upon identification. Subcontractor acknowledges that pre-existing work and all Work for Hire and other work product is subject to the FAR and DFARS clauses incorporated by reference herein.

D. In the event of any action for infringement of an enforceable intellectual property right including Patent, Trademark, and Copyright infringement, at a minimum, Subcontractor will, at Cadmus' direction: (a) obtain for Cadmus or Client the right to use the infringing material,

(b) modify the Work so as to render them non-infringing and functionally equivalent, (c) provide Cadmus with functionally equivalent substitute Work, or (d) pay for Cadmus to procure a non-infringing replacement Work. Any remedy under this paragraph shall be undertaken at the expense of the party that furnished the infringing material.

H.4 Changes

Neither this Agreement, nor any term, condition, or provision hereof, may be altered, changed, or modified in any manner whatsoever except upon the mutual agreement of both parties evidenced by a modification to the Agreement that is signed by both Subcontractor and Cadmus Contracts Department, with the exception of a unilateral modification by Cadmus. Such unilateral modifications are authorized to increase Ceiling Values, to increase or decrease funding, to issue incremental funding and/or Award Fee if applicable, to make changes in accordance with the Changes or other clauses in the Prime Contract or this Agreement, to issue line item corrections, terminations, and changes of a purely administrative natured Termination.

H.5 Notices

A. If Subcontractor encounters difficulty in meeting performance requirements, anticipates difficulty in complying with this Agreement's delivery schedule or dates, or has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Agreement; Subcontractor shall immediately notify Cadmus in writing, giving pertinent details. This notification shall be informational only, and compliance with this provision shall not be construed as a waiver by Cadmus of any delivery schedule or date or of any rights or remedies.

B. Any notice and similar communications concerning this Agreement ("Notice") shall be in writing, and shall be either (i) delivered in person, (ii) sent to the other party via electronic mail with electronic confirmation of receipt, or (iii) sent to the other party by certified mail with return receipt requested or by facsimile, electronically confirmed and followed up immediately by regular mail. Notices shall be delivered or sent to the parties' respective designees for Subcontract Administration, or to such other address as either party may hereafter establish by notice given in the manner prescribed in this paragraph. A Notice shall be considered given when delivered.

H.6 Communications with Client

Subcontractor is expressly prohibited from communicating with Client personnel with respect to management issues, pricing, payments, specific tasking, or Subcontractor's performance under tasks relating to the Prime Contract and/or this Agreement, without the prior consent of Cadmus. This restriction is not intended to interfere with Subcontractor's other contracts with the Client or normal sales outside the scope of this Agreement. Subcontractor may be expected to communicate directly with the technical client solely regarding technical progress of Subcontractor commissioned tasks and the Subcontractor has been authorized to start work, after receiving approval of Cadmus technical manager to do so. No privity of contract exists between Subcontractor and the Client, therefore Subcontractor may neither take direction from nor discuss any terms and conditions of this Agreement with Client without the written consent of Cadmus.

H.7 Stop Work and Termination

A. Stop Work. Cadmus may require that Subcontractor stop work on any or all work pursuant to this Agreement at any time by written notice to Subcontractor; such notice is effective upon receipt unless otherwise provided in the notification. In the event of work stoppage, Subcontractor shall immediately suspend the provision of Services. In the case of work stoppage, Subcontractor agrees to waive any claim for damages, including loss of anticipated profits.

B. Termination for Convenience. Cadmus may terminate this Agreement in whole or in part at any time by written notice to Subcontractor; such notice is effective upon receipt unless otherwise provided in the termination letter. In the event of such termination, Subcontractor shall immediately halt the provision of Services and Cadmus shall pay for all actual costs for authorized Work completed before the effective date of termination to the reasonable satisfaction of Cadmus.

C. Termination for Default. If Cadmus believes, in its sole discretion that (i) Subcontractor has failed to perform a material obligation under this Agreement, (ii) Subcontractor has failed to comply with any applicable laws, (iii) Subcontractor's performance threatens delivery under the Prime Contract (a "Breach"), or (iv) Subcontractor initiates any bankruptcy, insolvency, reorganization, readjustment of debt, dissolution, liquidation, or similar proceeding under the laws of any jurisdiction or any such proceeding is instituted against Subcontractor, then Cadmus shall provide written notice to Subcontractor describing the alleged Breach in reasonable detail and containing a reference to this Article. If the Subcontractor does not cure the Breach within that time designated in such written notice, then Cadmus may terminate the Agreement for cause by providing written notice to the Subcontractor. Notwithstanding the foregoing, Cadmus may terminate immediately upon notice of any breach under (ii) herein.

H.8 Force Majeure

Any delay of either party in the performance of its required obligations hereunder shall be excused to the extent caused by unprecedented weather conditions, fire, explosion, riot, war, court injunction or order, federal and/or state law or regulation, or order by any federal or state regulatory agency, but only to the extent that: 1) such events are beyond the reasonable control of the party affected, 2) such events were unforeseeable by the affected party and the effects were beyond its reasonable efforts to prevent, avoid or mitigate, 3) said affected party uses every reasonable effort to prevent, avoid or mitigate the effects, 4) prompt written notice of such delay be given by such affected party to the other; and 5) the party affected uses its best efforts to remedy the resulting effects in the shortest practicable time. If such circumstances should prevent or delay the performance of a party for thirty (30) days, the other party shall thereafter have the right to terminate the Agreement upon written notice at any time before such performance resumes.

H.9 Warranties

A. Subcontractor warrants that it has all rights necessary to fulfill the requirements of this Agreement, and that Subcontractor shall perform its services in accordance with this

Agreement in a manner consistent with the highest professional standards exercised by members of the same profession currently practicing under similar circumstances. Subcontractor shall be responsible for the professional quality, technical accuracy, completeness and coordination of the Work and other services furnished under the Agreement. Subcontractor warrants that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded for the award of contracts by any client.

B. Upon receipt of notice from Cadmus of any failure to comply with the terms of this Agreement or in respect to any defect within the Work, Subcontractor shall without additional compensation correct any such defects within a time acceptable to Cadmus and shall reimburse Cadmus for any resulting costs, expenses, or damages suffered by Cadmus, including, but not limited to, reprocurement or reperformance of the Work.

C. Subcontractor warrants that, at the time of delivery to Cadmus, the Deliverables will not infringe any Enforceable Intellectual Property Right of any third party. Subcontractor makes no warranty with respect to third party rights in any materials furnished to Subcontractor by Cadmus.

D. Subcontractor warrants that is shall comply with all applicable federal, state, and local laws and regulation in effect including, without limitation, the Procurement Integrity Act, 41 U.S.C. 423, and its implementing regulations. Subcontractor shall provide Cadmus with any information and/or certifications reasonably requested and related to its compliance with law or regulation.

H.10 Indemnity

A. Subcontractor shall indemnify Cadmus from and against any damages, costs or penalties and any payments (including without limitation fees, credits, refunds, costs, fines or penalties) incurred by Cadmus and resulting from Subcontractor's performance of its obligations hereunder or failure to perform, failure to comply with applicable laws or regulations, alleged infringement of third party intellectual property rights, or as a result of a breach by the Subcontractor of its obligations hereunder.

B. The obligations stated in this Article 2.10 shall not be limited in any way by the requirements of Article 2.12, Insurance, or by Subcontractor's actual insurance coverage.

H.11 Limitation of Liability

Except in the case of indemnification obligations, claims made by the U.S. Government or payments (including fines or penalties) made by Cadmus to the U.S. Government arising from Subcontractor's actions or failures to act, and/or breaches of confidentiality, in no event shall either party or its respective employees, representatives or subsidiaries be liable to the other party for any consequential, indirect, punitive, incidental or special damages, whether foreseeable or unforeseeable, and whether or not Subcontractor, Cadmus, or anyone else has been advised of the possibility of such damages.

H.12 Insurance

Without prejudice to Subcontractor's liability to indemnify Cadmus as stated in any Indemnification provision contained in this Agreement, Subcontractor shall procure at its

expense and maintain for the duration of this Agreement, and ensure that any of its subcontractors used in connection with this Agreement procure and maintain, the insurance policies required below with financially responsible insurance companies rated at least "A-" Class "VII" by A.M. Best's rating organization, and with policy limits not less than those indicated below.

(a) Workers' Compensation: Coverage for statutory obligations imposed by laws of any State in which the work is to be performed, including All State and Voluntary Compensation endorsement, and where applicable, coverage under the United States Longshoreman's and Harbor Workers' Act (USL&H), the Jones Act and the Defense Base Act (DBA). In addition, the policy shall be endorsed to waive the insurer's rights of subrogation in favor of Cadmus.

(b) Employer's Liability: Coverage for injuries to employees not covered by workers' compensation with limits of at least $1,000,000 each accident. The policy shall be endorsed to waive the insurer's rights of subrogation in favor of Cadmus.

(c) Mandatory Disability: Coverage required for disability benefits with statutory limits as required by the state, if work is being performed in a state where mandatory disability benefits are required.

(d) Commercial General Liability: Coverage for third party bodily injury and property damage, personal injury, premises operations, products and completed operations, personal and advertising injury, contractual liability, and independent contractors' liability with limits not less than $1,000,000 per occurrence and $2,000,000 in the aggregate. Cadmus, its officers and employees, and Cadmus's customers where required by Cadmus's Agreement with its customer, shall be named as Additional Insured and a waiver of subrogation shall be provided in favor of Cadmus.

(e) Business Automobile Liability: Coverage for use of all owned, non-owned, and hired vehicles with limits of not less than $1,000,000 per occurrence combined single limit for bodily injury and property damage liability. Cadmus, its officers and employees, and Cadmus's customers where required by Cadmus's Agreement with its customer, shall be named as Additional Insured and a waiver of subrogation shall be provided in favor of Cadmus.

(f) Professional Liability: If Subcontractor is performing any professional services, coverage for damages (including financial loss) caused by any acts, errors and omissions arising out Subcontractor's performance of professional services with limits of not less than $1,000,000 per claim and $2,000,000 in the aggregate.

(g) Umbrella liability policy with a limit of not less than $1,000,000 providing excess coverage over the underlying General Liability, Automobile Liability and Employers Liability coverages and limits stated above. Waiver of subrogation applies in favor of Cadmus for recovery of damages to the extent these damages are covered by the underlying General Liability, Employers Liability and Business Auto Liability policies maintained pursuant to this Agreement.

The required insurance coverages above shall be primary and non-contributing with respect to any other insurance that may be maintained by Cadmus and notwithstanding any provision

contained herein, the Subcontractor, and its employees, agents, representatives, consultants, subcontractors and suppliers, are not insured by Cadmus, and are not covered under any policy of insurance that Cadmus has obtained or has in place.

Any self-insured retentions, deductibles and exclusions in coverage in the policies required under this Article shall be assumed by, for the account of, and at the sole risk of Subcontractor or the subcontractor which provides the insurance and to the extent applicable shall be paid by Subcontractor or such subcontractor. In no event shall the liability of Subcontractor or any subcontractor be limited to the extent of any of insurance or the minimum limits required herein.

Subcontractor shall have all liability insurance required under this order amended or endorsed to name Cadmus as an additional insured and to indicate that, with respect to the additional insured, there shall be severability of interest. Prior to commencement of any work, and upon expiration of any policy renewal that occurs while any work is on-going under this Agreement, Subcontractor shall provide Cadmus certificates of insurance evidencing the insurance policies above, including evidence of additional insured status and waivers of subrogation where required. Cadmus reserves the right to refuse to accept policies from companies with an A.M. Best rating of less than A- VII. Subcontractor or its insurers, shall provide 30 days' advance written notice to Cadmus in the event of cancellation or material modification of any policy. Failure of Cadmus to demand such certificates or to identify any deficiency in the insurance provided shall not be construed as or deemed to be a waiver of Subcontractor's, or its subcontractors', obligations to maintain the above insurance coverages.

H.13 Claims Related to Prime Contracts

If a final decision is made by the Contracting Officer of Client, and such final decision pertains to the subject matter of this Subcontract, then such final decision shall be binding upon Subcontractor with respect to such matter, except that Subcontractor's rights of appeal through a Cadmus sponsored claim are available to Subcontractor. If Subcontractor desires Cadmus to bring a claim on its behalf, Subcontractor shall timely submit a written request to Cadmus setting forth the legal basis of the claim, along with any required certifications. If Cadmus elects to bring the claim on the Subcontractor's behalf, the Subcontractor shall cooperate with Cadmus in the preparation of the claim and be responsible for all costs. If, as a result of any final decision or appeal thereof, Cadmus is unable to obtain payment, or reimbursement, from Client, or is required to refund, or credit, to Client any amount with respect to any item, or matter, for which Cadmus has reimbursed, or paid, to Subcontractor, then Subcontractor shall, on demand, promptly repay such amount to Cadmus. Cadmus' maximum liability to Subcontractor for any matter connected with, or related to, this Subcontract which was properly the subject of a final decision, or appeal, thereof is the amount of Cadmus' recovery from the Client for that claim. Except as may be expressly set forth in this Agreement with the Government Contracting Officer's express consent, Subcontractor shall not acquire any direct claim or direct course of action against the US Government.

H.14 Independent Relationship.

Subcontractor and Cadmus shall at all times be independent parties. Neither party is an employee, joint venturer, agent, or partner of the other; neither party is authorized to assume or create any obligations or liabilities, express or implied, on behalf of or in the name of the other. The employees, methods, facilities and equipment of each party shall at all times be under the exclusive direction and control of that party.

H.15 Nonwaiver.

A. Neither party shall be deemed to have waived any right or remedy unless such waiver is made expressly and in writing

B. The failure by Cadmus to require strict conformance to any provision in this Subcontract shall not affect Cadmus' right to require performance at any time thereafter, nor shall a waiver of any breach or default of this Subcontract constitute a waiver of any subsequent breach or default or a waiver of the provision itself.

H.16 Assignment and Subcontracting

Neither this Agreement nor any duty or right under this Agreement shall be delegated or assigned by Subcontractor to another party without the prior written consent of Cadmus, except that claims for monies due or to become due may be assigned to a financial institution if Cadmus is so notified in writing prior to such assignment. Cadmus shall be furnished a signed copy of any such assignment. All payments under this Agreement, including those to an assignee, shall be subject to setoff or recoupment for any present or future claim or claims that Cadmus may have against Subcontractor. Cadmus reserves the right to make settlements, or adjustments in price, or both, with Subcontractor under the terms of this Agreement notwithstanding any assignment of claims for monies due or to become due hereunder and without notice to the assignee. Subcontractor is responsible to ensure that all terms, conditions and flow-down requirements in this Agreement are flowed down to any lower tier subcontractor who is approved by Cadmus. Subcontractor is fully responsible for the acts and omissions of its lower tier subcontractors and of persons either directly or indirectly employed by them.

H.17 Export Control

Subcontractor shall comply with all applicable U.S. export laws and regulation, including International Traffic in Arms Regulation ("ITAR") and the Export Administration Regulations ("EAR"). The subcontract technology of this Agreement, including data, services, software and hardware provided hereunder, may be controlled under these laws and regulations and may not be exported or re-exported without prior authorization in accordance with ITAR and EAR. Without limiting the foregoing, Subcontractor agrees that it will not transfer any export controlled item, data, or services, to include transfer to foreign persons employed by or associated with, or under contract to Subcontractor or Subcontractor's lower-tier suppliers, without the authority of an export license, agreement, or applicable exemption or exception. Additionally, Subcontractor agrees that to the extent applicable, it will comply with the requirements of the then-current version of the General Data Protection Regulation (GDPR). Subcontractor further represents and warrants that it will not take any actions that will compromise Cadmus' ability to comply with the GDPR.

H.18 Non-Solicitation

Unless otherwise agreed to in writing, during the term of this Agreement and for a period of one (1) year after the expiration or termination of this Agreement, Subcontractor shall not knowingly solicit for employment any person employed Cadmus working under this Agreement. This Article shall not restrict in any way the right of either party to solicit or recruit generally in the media, and shall not prohibit Subcontractor from hiring an employee of Cadmus who answers any

advertisement or who otherwise voluntarily applies for hire without having been personally solicited by Subcontractor.

H.19 Entire Agreement.

This Agreement, together with its Sections, Exhibits, NDA, and Amendments, executed by the parties, constitutes the entire agreement of the parties, superseding all prior agreements and understandings as to the subject matter herein. No reliance may be placed on any warranty, representation, opinion, advice or assertion of fact made either prior to, contemporaneous with, or after entering into this Agreement, except to the extent that it has been reduced to writing and included as a term of the Agreement. All work performed by Subcontractor, actions taken, and payments made, if any, under any other prior written oral agreements, with respect to this Agreement, shall be deemed to have been work performed, actions taken, or payments made under this Agreement. None of the parties to the Agreement have been induced to enter into the Agreement or any amendment or supplement by reason of any such warranty, representation, opinion, advice or assertion of fact.

H.20 Governing Law.

Interpretation, construction and enforcement of this Agreement shall be pursuant to the laws, statutes and regulations of the Commonwealth of Massachusetts.

H.21 Severability.

If any provision of this Agreement is found invalid or unenforceable by a court of law or an arbitration panel, the remainder of this Agreement shall continue in full force and effect. If any provision of this Agreement is found invalid or unenforceable by a court of law or an arbitration panel, the Parties shall endeavor to modify that clause in a manner which gives effect to the intent of the Parties in entering into this Agreement.

H.22 Survival of Agreement.

Standard terms, which by their nature and intent, may continue beyond the termination of this Agreement, shall survive the termination of this Agreement. All provisions of this Agreement allocating liability between the Subcontractor, Client and Cadmus shall survive the termination of this Agreement.

H.23 Order of Precedence.

Any inconsistency in this Agreement shall be resolved by giving precedence in the following order:

1. Section 1.0: Schedule
2. Section 2.0: General Provisions
3. Section 3.0: Government Provisions
4. Section 4.0: Statement of Work & Invoice Schedule
5. Section 5.0: Supplemental Provisions
6. Section 6.0: Attachments

H.24 Limitation On Acquisition Of Information Technology (APRIL 2018) (DEVIATION Nos M/OAA-DEV-FAR-20-3c and M/OAA-DEV-AIDAR-20-2c) (APRIL 2020)

(a) Definitions. As used in this contract -- “Information Technology” means

(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term " information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts that include information technology or information technology services.

(c) The Contractor must not acquire information technology as defined in this clause without the prior written approval by the contracting officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology will be necessary to meet the Government’s requirements or to facilitate activities in the Government’s statement of work, the Contractor must request prior written approval from the Contracting Officer.

(2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must simultaneously notify the Contracting Officer’s Representative (COR) and the Office of the Chief Information Officer at ITAuthorization@usaid.gov.

(3) The Contracting Officer will provide written approval to the Contractor through modification to the contract expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. The Contracting Officer will include the applicable clauses and special contract requirements in the modification.

(e) Except as specified in the contracting officer’s written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for information technology as defined in this clause.

(f) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

[End of Clause]

H.25 AIDAR 752.228-3 Worker's Compensation Insurance (Defense Base Act) (DEC 1991) [(DEVIATION JUN 2022)] Class Deviation No. M-OAA-DEV-AIDAR-22-10c

In addition to the requirements specified in (48 CFR) FAR 52.228-3, the Contractor agrees to the following:

(a) The Contractor agrees to procure Defense Base Act (DBA) insurance pursuant to the terms of the contract between USAID and USAID's DBA insurance carrier unless the Contractor has a DBA self insurance program approved by the Department of Labor or has an approved retrospective rating agreement for DBA. The rates and contact information for USAID's DBA insurance carrier are published in an Acquisition & Assistance Policy Directive found on USAID's website: https://www.usaid.gov/work-usaid/resources-for-partners. Alternatively, the Contractor can request the rates and contact information from the Contracting Officer.

(b) If USAID or the Contractor has secured a waiver of DBA coverage (see (48 CFR) AIDAR 728.305-70(a)) for Contractor's employees who are not citizens of, residents of, or hired in the United States, the Contractor agrees to provide such employees with worker's compensation benefits as required by the laws of the country in which the employees are working, or by the laws of the employee's native country, whichever offers greater benefits.

(c) The Contractor further agrees to insert in all subcontracts hereunder to which the DBA is applicable, a clause similar to this clause, including this sentence, imposing on all subcontractors alike requirement to provide overseas worker's compensation insurance coverage and obtain DBA coverage under the USAID requirements contract.

H.26 PROHIBITION OF ASSISTANCE TO DRUG TRAFFICKERS

USAID reserves the right to terminate this Contract, to demand a refund or take other appropriate measures if the Contractor or sub awardees are found to have been convicted of a narcotics offense or to have been engaged in drug trafficking as defined in 22 CFR Part 140.

H.27 Contractor Access to USAID Facilities and USAID's Information Systems (APRIL 2018)) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) HSPD-12 and Personal Identity Verification (PIV). Individuals engaged in the performance of this award as employees, consultants, or volunteers of the contractor must comply with all applicable Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV) procedures, as described below, and any subsequent USAID or Government-wide HSPD-12 and PIV procedures/policies.

(b) A U.S. citizen or resident alien engaged in the performance of this award as an employee, consultant, or volunteer of a U.S firm may obtain access to USAID facilities or logical access to USAID's information systems only when and to the extent necessary to carry out this

award and in accordance with this clause. The contractor's employees, consultants, or volunteers who are not U.S. citizens or resident aliens as well as employees, consultants, or volunteers of non-U.S. firms, irrespective of their citizenship, will not be granted logical access to U.S. Government information technology systems (such as Phoenix, GLAAS, etc.) and must be escorted to use U.S. Government facilities (such as office space).

(c) (1) No later than five business days after award, the Contractor must provide to the Contracting Officer's Representative (COR) a complete list of employees that require access to USAID facilities or information systems.

(2) Before a contractor (or a contractor employee, consultant, or volunteer) or subcontractor at any tier may obtain a USAID ID (new or replacement) authorizing the individual routine access to USAID facilities in the United States, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form to the Enrollment Office personnel when undergoing processing. One identity source document must be a valid Federal or State Government-issued picture ID. Contractors may contact the USAID Security Office to obtain the list of acceptable forms of documentation. Submission of these documents, to include documentation of security background investigations, is mandatory in order for the Contractor to receive a PIV/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment.

(d) The Contractor must send a staffing report to the COR by the fifth day of each month. The report must contain the listing of all staff members with access that separated or were hired under this contract in the past sixty (60) calendar days. This report must be submitted even if no separations or hiring occurred during the reporting period. Failure to submit the 'Contractor Staffing Change Report' each month may, at USAID's discretion, result in the suspension of all logical access to USAID information systems and/or facilities access associated with this contract. USAID will establish the format for this report.

(e) Contractor employees are strictly prohibited from sharing logical access to USAID information systems and Sensitive Information. USAID will disable accounts and revoke logical access to USAID IT systems if Contractor employees share accounts.

(f) USAID, at its discretion, may suspend or terminate the access to any systems and/or facilities when a potential Information Security Incident or other electronic access violation, use, or misuse incident gives cause for such action. The suspension or termination may last until such time as USAID determines that the situation has been corrected or no longer exists.

(g) The Contractor must notify the COR and the USAID Service Desk at least five business days prior to the Contractor employee's removal from the contract. For unplanned terminations of Contractor employees, the Contractor must immediately notify the COR and the USAID Service Desk (CIOHELPDESK@usaid.gov or (202) 712-1234). The Contractor or its Facilities Security Officer must return USAID PIV/FAC cards and remote authentication tokens issued to Contractor employees to the COR prior to departure of the employee or upon completion or termination of the contract, whichever occurs first.

(h) The contractor is required to insert this clause including this paragraph (h) in any subcontracts that require the subcontractor, subcontractor employee, or consultant to have routine physical access to USAID space or logical access to USAID's information systems.

(End of Clause)

H.28 Restrictions Against Disclosure (MAY 2016) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) The Contractor agrees, in the performance of this contract, to keep the information furnished by the Government or acquired/developed by the Contractor in performance of the contract and designated by the Contracting Officer or Contracting Officer's Representative, in the strictest confidence. The Contractor also agrees not to publish or otherwise divulge such information, in whole or in part, in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Contractor's possession, to those employees needing such information to perform the work described herein, i.e., on a “need-to-know” basis. The Contractor agrees to immediately notify the Contracting Officer in writing in the event that the Contractor determines or has reason to suspect a breach of this requirement has occurred.

(b) All Contractor staff working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

(c) The Contractor shall insert the substance of this special contract requirement, including this paragraph (c), in all subcontracts when requiring a restriction on the release of information developed or obtained in connection with performance of the contract.

(End)

H.29 Information Technology Approval (APRIL 2018) (DEVIATION NO. M-OAA-DEV-FAR-22-03c)

(a) Definitions. As used in this contract -- “Information Technology” means

(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term " information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (OMB M-15-14)

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts or interagency agreements for information technology or information technology services.

(c) The approved information technology and/or information technology services are specified in the Schedule of this contract. The Contractor must not acquire additional information technology without the prior written approval of the Contracting Officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology in addition to that information technology specified in the Schedule will be necessary to meet the Government's requirements or to facilitate activities in the Government's statement of work, the Contractor must request prior written approval from the Contracting Officer.

(2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must simultaneously notify the Contracting Officer's Representative (COR) and the Office of the Chief Information Officer at ITAuthorization@usaid.gov.

(e) The Contracting Officer will provide written approval to the Contractor expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. Additional clauses or special contract requirements may be applicable and will be incorporated by the Contracting Officer through a modification to the contract.

(f) Except as specified in the Contracting Officer's written approval, the Government is not obligated to reimburse the Contractor for costs incurred in excess of the information technology equipment, software or services specified in the Schedule.

(g) The Contractor shall insert the substance of this special contract requirement, including this paragraph (g), in all subcontracts.

(End)

H.30 Media and Information Handling and Protection (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Definitions. As used in this special contract requirement- "Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. This also includes but not limited to all records, files, and metadata in electronic or hardcopy format.

"Sensitive Information or Sensitive But Unclassified" (SBU) means information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to:

1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and

2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers "Media" means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

(b) This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Handling and Protection. The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. The Contractor must develop and implement policies or documentation regarding the protection, handling, and destruction of Sensitive Information. The policy or procedure must address at a minimum, the requirements documented in NIST 800-53 Revision 4 or the current revision for Media Protection Controls as well as the following:

1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents

2) Proper security, control, and storage of mobile technology, portable data storage devices, and communication devices.

3) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information while at rest and in transit throughout USAID, contractor, and/or subcontractor networks, and on host and client platforms.

4) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

(d) Return of all USAID Agency records. Within five (5) business days after the expiration or termination of the contract, the contractor must return all Agency records and media provided by USAID and/or obtained by the Contractor while conducting activities in accordance with the contract.

(e) Destruction of Sensitive Information: Within twenty (20) business days after USAID has received all Agency records and media, the Contractor must execute secure destruction (either by the contractor or third party firm approved in advance by USAID) of all remaining originals and/or copies of information or media provided by USAID and/or obtained by the Contractor while conducting activities in accordance with the contract. After the destruction of all information and media, the contractor must provide USAID with written confirmation verifying secure destruction.

(f) The Contractor shall include the substance of this special contract requirement in all subcontracts, including this paragraph (f).

(End)

H.31 Privacy and Security Information Technology Systems Incident Reporting (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Definitions. As used in this special contract requirement- “Information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. “Sensitive Information” or “Sensitive But Unclassified” Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers, “Personally Identifiable Information (PII)”, means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an

individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term “individual” refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

“National Security Information” means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified or national security information is specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

“Information Security Incident” means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

“Spillage” means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited,(i.e., authorized) for the applicable security level of the data or information.

“Privacy Incident” means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of Personally Identifiable Information (PII), whether in electronic or paper format.

(b) This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as “Contractor”) and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Privacy Act Compliance

Contractors must comply with the Privacy Act of 1974 requirements in the design, development, or operation of any system of records on individuals (as defined in FAR) containing PII developed or operated for USAID or to accomplish a USAID function for a System of Records (SOR).

(d) IT Security and Privacy Training

(1) All Contractor personnel must complete USAID-provided mandatory security and privacy training prior to gaining access to USAID information systems and annually thereafter.

(2) The USAID Rules of Behavior and all subsequent updates apply to and must be signed by each user prior to gaining access to USAID facilities and information systems, periodically at the request of USAID. USAID will provide access to the rules of behavior and provide notification as required.

(3) Security and privacy refresher training must be completed on an annual basis by all contractor and subcontractor personnel providing support under this contract. USAID will provide notification and instructions on completing this training.

(4) Contractor employees filling roles identified by USAID as having significant security responsibilities must complete role-based training upon assignment of duties and thereafter at a minimum of every three years.

(5) Within fifteen (15) calendar days of completing the initial IT security training, the contractor must notify the COR in writing that its employees, in performance of the contract, have completed the training. The COR will inform the contractor of any other training requirements.

(e) Information Security and Privacy Incidents

(1) Information Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.

(i) Contractor employees must report by e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the Contracting Officer and Contracting Officer's representative and the Contractor Facilities Security Officer.

Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Contractor's discovery of a spillage or security incident involving classified information, the Contractor must immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or security incident in compliance with agency-specific instructions. The Contractor will abide by USAID instructions on correcting such a spill or security incident.

Contractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Contractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

(ii) The Contractor must provide any supplementary information or reports related to a previously reported incident directly to CIO-HELPDESK@usaid.gov, upon request.

Correspondence must include related ticket number(s) as provided by the USAID Service Desk with the subject line “Action Required: Potential Security Incident”.

(2) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information (PII), and can result in the loss of the public's trust and confidence in the Agency’s ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Contractor employees must report (by e-mail) all Privacy Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the incident, at:

CIO-HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer’s representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read “Action Required: Potential Privacy Incident”.

(3) Information Security Incident Response Requirements

(i) All determinations related to Information Security and Privacy Incidents, associated with information Systems or Information maintained by the contractor in support of the activities authorized under this contract, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by USAID officials (except reporting criminal activity to law enforcement). The Contractor must not conduct any internal information security incident-related review or response activities that could modify or eliminate any existing technical configuration or information or forensic technical evidence existing at the time of the information security incident without approval from the Agency CIO communicated through the CO or COR.

(ii) The Contractor and contractor employees must provide full and immediate access and cooperation for all activities USAID requests to facilitate Incident Response, including providing all requested images, log files, and event information to address and resolve Information Security Incidents.

(iii) Incident Response activities that USAID requires may include but are not limited to, inspections; investigations; forensic reviews; data analyses and processing.

(iv) At its discretion, USAID may obtain the assistance of Federal agencies and/or third party firms to aid in Incident Response activities.

(v) All determinations related to an Information Security Incident associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract will be made only by the USAID CIO through the CO or COR.

(vi) The Contractor must report criminal activity to law enforcement organizations upon becoming aware of such activity.

(f) The Contractor shall immediately notify the Contracting Officer in writing whenever it has reason to believe that the terms and conditions of the contract may be affected as a result of the reported incident.

(g) The Contractor is required to include the substance of this provision in all subcontracts. In altering this special contract requirement, require subcontractors to report (by e-mail) information security and privacy incidents directly to the USAID Service Desk at CIO-HELPDESK@usaid.gov. A copy of the correspondence shall be sent to the prime Contractor (or higher tier subcontractor) and the Contracting Officer referencing the ticket number provided by the CIO-HELPDESK.

(End)

H.32 Security Requirements for Unclassified Information Technology Resources (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Definitions. As used in this special contract requirement-

“Audit Review” means the audit and assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities and methods for mitigating them and assist in implementation of new security controls where required. These reviews are conducted periodically but at least annually, and may be performed by USAID Bureau for Management, Office of the Chief Information Officer (M/CIO) or designated independent assessors/auditors, USAID Office of Inspector General (OIG) as well as external governing bodies such as the Government Accountability Office (GAO).

“Authorizing Official” means the authorizing official is a senior government official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and/or the Nation.

“Information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

“Sensitive” Information or Sensitive But Unclassified (SBU) - Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. “National Security Information” means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified or national security information is specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

"Information Technology Resources" means agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants to third parties which establish or support information technology not operated directly by the Federal Government. (OMB M-15-14)

(b) Applicability: This special contract requirement applies to the Contractor, its subcontractors, and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Compliance with IT Security and Privacy Policies: The contractor shall be responsible for implementing information security for all information systems procured, developed, deployed, and/or operated on behalf of the US Government. All Contractor personnel performing under this contract and Contractor equipment used to process or store USAID data, or to connect to USAID networks, must comply with Agency information security requirements as well as current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA), Privacy Act of 1974, E-Government Act of 2002, Section 208, and National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other relevant Federal laws and regulations that are applicable to USAID. The Contractor must comply with the following:

(1) HSPD-12 Compliance

(i) Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.

(ii) All development for USAID systems must include requirements to enable the use Personal Identity Verification (PIV) credentials, in accordance with NIST FIPS 201, PIV of Federal Employees and Contractors, prior to being operational or updated.

(2) Internet Protocol Version 6 (IPv6) or current version: This acquisition requires all functionality, capabilities and features to be supported and operational in both a dual-stack IPv4/IPv6 environment and an IPv6 only environment. Furthermore, all management, user interfaces, configuration options, reports and other administrative capabilities that support IPv4 functionality will support comparable IPv6 functionality. The Contractor is required to certify that its products have been tested to meet the requirements for both a dual-stack

IPv4/IPv6 and IPv6-only environment. USAID reserves the right to require the Contractor's products to be tested within a USAID or third party test facility to show compliance with this requirement.

(3) Secure Configurations

(i) The Contractor's applications must meet all functional requirements and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB) or the current configuration baseline.

(ii) The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration. The information technology, when applicable, must also use the Windows Installer Service for installation to the default "program files" directory and must be able to silently install and uninstall.

(iii) Applications designed for normal end users must run in the standard user context without elevated system administration privileges.

(iv) The Contractor must apply due diligence at all times to ensure that the required level of security is always in place to protect USAID systems and information, such as using Defense Information Systems Agency Security Technical Implementation Guides (STIGs), common security configurations available from the National Institute of Standards and Technology's website at https://nvd.nist.gov/ncp/repository or USAID established configuration settings.

(4) FIPS 140 Encryption Requirements: Cryptographic modules used to protect USAID information must be compliant with the current FIPS 140 version and validated by the Cryptographic Module Validation Program (CMVP). The Contractor must provide the validation certificate number to USAID for verification. The Contractor is required to follow government-wide (FIPS 140) encryption standards.

(5) Security Monitoring, Auditing and Alerting Requirements: All Contractor-owned and operated systems that use or store USAID information must meet or exceed standards documented in this contract and in Service Level Agreements and Memorandums of Understanding/Agreements pertaining to security monitoring and alerting. These requirements include but are not limited to:

System and Network Visibility and Policy Enforcement at the following levels:

- Edge
- Server / Host
- Workstation / Laptop / Client
- Network
- Application
- Database
- Storage
- User
- Alerting and Monitoring
- System, User, and Data Segmentation

(6) Contractor System Oversight/Compliance

(i) The federal government has the authority to conduct site reviews for compliance validation. Full cooperation by the Contractor is required for audits and forensic analysis.

(ii) The Contractors must afford USAID the level of physical or logical access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases to the extent required to support its security and privacy programs. This includes monitoring, inspection, investigation and audits to safeguard against threats and hazards to the integrity, availability and confidentiality of USAID data or information systems operated on behalf of USAID; and to preserve or retrieve evidence in the case of computer crimes.

(iii) All Contractor systems must comply with Information Security Continuous Monitoring (ISCM) and Reporting as defined in a continuous monitoring plan, to include, but not limited to, both automated authenticated and unauthenticated scans of networks, operating systems, applications, and databases. The Contractor must provide a continuous monitoring plan in accordance with NIST standards, as well as scan results upon request or at a minimum monthly to the Contracting Officer Representative (COR) and Contracting Officer, in addition to the CIO at ITAuthorization@usaid.gov. Alternatively, the Contractor may allow USAID information security staff to run scans directly.

(iv) The Contractors must comply with systems development and lifecycle management best practices and processes as defined by Bureau for Management, Office of The Chief Information Officer (M/CIO) USAID IT Project Governance standards and processes for approval of IT projects, for the acceptance of IT project deliverables, and for the project's progression through its life cycle.

(7) Security Assessment and Authorization (SA&A)

(i) For all information systems procured, developed, deployed, and/or operated on behalf of the US Government information by the provision of this contract, the Contractor must provide a system security assessment and authorization work plan, including project management information, to demonstrate that it complies or will comply with the FISMA and NIST requirements. The work plan must be approved by the COR, in consultation with the USAID M/CIO Information Assurance Division.

(ii) Prior to deployment of all information systems that transmit, store or process Government information, the contractor must obtain an Authority to Operate (ATO) signed by a USAID Authorizing Official from the contracting officer or COR. The Contractor must adhere to current NIST guidance for SA&A activities and continuous monitoring activities thereafter.

(iii) Prior to the SA&A, a Privacy Threshold Analysis (PTA) must be completed using the USAID Privacy Threshold Analysis Template. The completed PTA must be provided to the USAID Privacy Officer or designate to determine if a Privacy Impact Analysis (PIA) is required. If a determination is made that a PIA is required, it must be completed in accordance with the USAID PIA Template, which USAID will provide to the Contractor as necessary. All privacy requirements must be completed in coordination with the COR or other designated Government staff.

(iv) Prior to the Agency security assessment, authorization and approval, the Contractor must coordinate with the COR and other Government personnel as required to complete the FIPS 199 Security categorization and to document the systems security control baseline.

(v) All documentation must be prepared, stored, and managed in accordance with standards, templates and guidelines established by USAID M/CIO. The USAID M/CIO or designee must approve all SA&A requirements.

(vi) In information systems owned or operated by a contractor on behalf of an agency, or for information collected or maintained by or on behalf of the agency, an SA&A must be done independent of USAID, to include the selection of a Federal Risk and Authorization Management Program (FEDRAMP) approved independent Third Party Assessor (3PAO). See approved list of Assessors at https://www.fedramp.gov/ /. The Contractor must submit a signed SA&A package approved by the 3PAO to USAID at saacapackages@usaid.gov at least 60 calendar days prior to obtain the ATO for the IT system.

(vii) USAID retains the right to deny or rescind the ATO for any system if it believes the package or system fails to meet the USAID security requirements. Moreover, USAID may or may not provide general or detailed guidance to the Contractor to improve the SA&A package or the overall security posture of the information system and may or may not require re-submission of the package upon completion of the modifications. USAID reserves the right to limit the number of resubmissions at its convenience and may determine a system's compliance to be insufficient at which time a final determination will be made to authorize or deny operation. USAID is the final authority on the compliance.

(viii) The Contractor must submit SA&A packages to the CIO at least sixty (60) days prior to production or the expiration of the current ATO.

(ix) Once the USAID Chief Information Security Officer or designee determines the risks, the Contractor must ensure that all Plan of Action and Milestones resulting from security assessments and continuous monitoring are remediated within a time frame commensurate with the level of risk as follows:

- High Risk = 30 calendar days;
- Moderate Risk = 60 calendar days; and
- Low Risk = 180 calendar days

(8) Federal Reporting Requirements: Contractors operating information systems on behalf of USAID must comply with FISMA reporting requirements. Monthly, quarterly and annual data collections will be coordinated by USAID. Data collections include but are not limited to, data feeds in a format consistent with Office of Management and Budget (OMB) requirements. The Contractor must provide timely responses as requested by USAID and OMB.

(d) The Contractor shall include the substance of this special contract requirement, including this paragraph (d), in all subcontracts, including subcontracts for commercial items.

(End)

H.33 Cloud Computing (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Definitions. As used in this special contract requirement-

“Cloud computing” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"Federal information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government, in any medium or form. (OMB A-130)
“Information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

“Information Security Incident” means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

“Privacy Incident means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of Personally Identifiable Information (PII), whether in electronic or paper format.

“Spillage” means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited,(i.e., authorized) for the applicable security level of the data or information.

“Cloud Service Provider” or CSP means a company or organization that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

“Penetration Testing” means security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. (NIST SP 800- 115)

“Third Party Assessment Organizations” means an organization independent of the organization whose IT system is being assessed. They are required to meet the ISO/IEC 17020:1998 standards for independence and managerial competence and meet program requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions.

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to

identify an individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term "individual" refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

(b) Applicability

This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Limitations on access to, use and disclosure of, Federal information.

(1) The Contractor shall not access, use, or disclose Federal information unless specifically authorized by the terms of this contract issued hereunder.

(i) If authorized by the terms of this contract issued hereunder, any access to, or use or disclosure of, Federal information shall only be for purposes specified in this contract.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall remain effective beyond the expiration or termination of this contract.

(2) The Contractor shall use related Federal information only to manage the operational environment that supports the Federal information and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) Records Management and Access to Information

(1) The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with capabilities such as those identified in the provisions of this contract and National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Federal information, including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by the Contracting Officer in support of government compliance requirements to include but not limited to Freedom of Information Act, Privacy Act, e-Discovery, eRecords and legal or security investigations.

(3) The Contractor shall retain and maintain all Federal information in accordance with records retention provisions negotiated by the terms of the contract and in accordance with USAID records retention policies.

(4) The Contractor shall dispose of Federal information in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(e) Notification of third party access to Federal information : The Contractor shall notify the Government immediately of any requests from a third party for access to Federal information or, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or Local agency, that could result in the disclosure of any Federal information to a third party. The Contractor shall cooperate with the Government to take all measures to protect Federal information, from any loss or unauthorized disclosure that might reasonably result from the execution of any such request, warrant, seizure, subpoena, or similar legal process.

(f) Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Contractor's discovery of a spillage or security incident involving classified information, the Contractor shall immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or information security incident in compliance with agency-specific instructions. The Contractor will also notify the Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer. The Contractor will abide by USAID instructions on correcting such a spill or information security incident. For all spills and information security incidents involving unclassified and/or SBU information, the protocols outlined above in section (g) and (h) below shall apply.

(g) Information Security Incidents

(1) Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the information security incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.

(i) Contractor employees must report via e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the Contracting Officer and Contracting Officer's representative and the Contractor Facilities Security Officer. Contractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Contractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

(ii) The Contractor must provide any supplementary information or reports related to a previously reported information security incident directly to CIO-HELPDESK@usaid.gov,

upon request. Correspondence must include related ticket number(s) as provided by the USAID Service Desk with the subject line “Action Required: Potential Security Incident”.

(h) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information, and can result in the loss of the public's trust and confidence in the Agency’s ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Contractor employees must report by e-mail all Privacy Incidents to the USAID Service Desk immediately (within 30 minutes), after becoming aware of the Incident, at: CIO-HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer’s representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read “Action Required: Potential Privacy Incident”.

(i) Information Ownership and Rights: USAID information stored in a cloud environment remains the property of USAID, not the Contractor or cloud service provider (CSP). USAID retains ownership of the information and any media type that stores Federal information. The CSP shall only use the Federal information for purposes explicitly stated in the contract. Further, the cloud service provider shall export Federal information in a machine-readable and non-proprietary format that USAID requests at the time of production, unless the parties agree otherwise.

(j) Security Requirements:

(1) The Contractor shall adopt and maintain administrative, technical, operational, and physical safeguards and controls that meet or exceed requirements contained within the Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline, current standard for NIST 800-53 (Security and Privacy Controls for Federal Information Systems) and Organizations, including Appendix J, and FedRAMP Continuous Monitoring Requirements for the security level and services being provided, in accordance with the security categorization or impact level as defined by the government based on the Federal Information Processing Standard (FIPS) Publication 199 (FIPS-199).

(2) The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the security assessment and authorization (SA&A) is based on the system’s complexity and security categorization. The Contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.FedRAMP.gov.

(3) The Contractor must support SA&A activities to include assessment by an accredited Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system’s security posture in accordance with the FedRAMP Continuous Monitoring Plan. The Contractor must make available to the Contracting Officer, the most current, and any other, Security Assessment Reports for consideration as part of the Contractor’s overall Systems Security Plan.

(4) The Government reserves the right to perform penetration testing or request Penetration Testing by an independent source. If the Government exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems, web applications, databases, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Federal information for vulnerabilities.

(5) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report must be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.

(6) The Contractor is responsible for mitigating all security risks found during SA&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within thirty (30) calendar days and all moderate risk vulnerabilities must be mitigated within sixty (60) calendar days from the date vulnerabilities are formally identified. USAID may revoke an ATO for any system if it is determined that the system does not comply with USAID standards or presents an unacceptable risk to the Agency. The Government will determine the risk rating of vulnerabilities.

(7) The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements and to allow for appropriate risk decisions for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The Contractor must make appropriate personnel available for interviews and provide all necessary documentation during this review and as necessary for continuous monitoring activities.

(k) Privacy Requirements: Cloud Service Provider (CSP) must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect Personally Identifiable Information (PII) about individuals that will be collected and maintained by the Contractor solution. The Contractor responsibilities include full cooperation for any request for disclosure, subpoena, or other judicial process seeking access to records subject to the Privacy Act of 1974.

(l) Data Location: The Contractor must disclose the data server locations where the Agency data will be stored as well as the redundant server locations. The Contractor must have prior Agency approval to store Agency data in locations outside of the United States.

(m) Terms of Service (ToS): The Contractor must disclose any requirements for terms of service agreements and clearly define such terms prior to contract award. All ToS provisions regarding controlling law, jurisdiction, and indemnification must align with Federal statutes, policies, and regulations.

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; clearly define how performance is guaranteed (such as response time

resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have been resolved or mitigated. Additionally, at USAID's request, the Contractor must submit reports or provide a dashboard where USAID can continuously verify that service levels are being met. Where SLAs fail to be met, USAID may assess monetary penalties or service credit.

(o) Trusted Internet Connection (TIC): The Contractor must route all USAID traffic through the TIC.

(p) Forensics, Freedom of Information Act (FOIA), Electronic Discovery, or additional Information Requests: The Contractor must allow USAID access required to retrieve information necessary for FOIA and Electronic Discovery activities, as well as, forensic investigations for both criminal and noncriminal purposes without their interference in these activities. USAID may negotiate roles and responsibilities for conducting these activities in agreements outside of this contract.

(1) The Contractor must ensure appropriate forensic tools can reach all devices based on an approved timetable.

(2) The Contractor must not install forensic software or tools without the permission of USAID.

(3) The Contractor, in coordination with USAID Bureau for Management, Office of The Chief Information Officer (M/CIO)/ Information Assurance Division (IA), must document and preserve data required for these activities in accordance with the terms and conditions of the contract.

(4) The Contractor, in coordination with USAID M/CIO/IA, must clearly define capabilities, procedures, roles and responsibilities and tools and methodologies for these activities.

(q) The Contractor shall include the substance of this special contract requirement, including this paragraph (p), in all subcontracts, including subcontracts for commercial items.

(End)

[End of Section H]

PART II – CONTRACT CLAUSES

I. CONTRACT CLAUSES

Section I and its contents here within are only applicable to the USAID portion of funding.

FAR

52.202-1	Definitions
52.203-5	Covenant Against Contingent Fees
52.203-6	Restrictions on Subcontractor Sales to the Government
52.203-8	Cancellation, rescission, and Recovery of Funds for illegal or Improper Activity
52.203-17	Contractor Employee Whistleblower Rights
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements
52.204-6	Unique Entity Identifier (applicable if exceeds $30,000)
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
52.204-26	Covered Telecommunications Equipment or Services— Representation
52.204-27	Prohibition on a ByteDance Covered Application
52.204-30	Federal Acquisition Supply Chain Security Act Orders—Prohibition
52.209-6	Protecting the Government's Interest when Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (applicable only if exceeds $35,000)
52.215-2	Audit and Records - Negotiation (applicable only if exceeds $150,000)
52.222-2	PAYMENT FOR OVERTIME PREMIUMS
52.222-3	Convict Labor
52.222-21	Prohibition of Segregated Facilities
52.222-26	Equal Opportunity (applicable only if US subcontractor/vendor)

52.222-36	Equal Employment for Workers with Disabilities
52.222-37	EMPLOYMENT REPORTS ON VETERANS
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT
52.222-41	Service Contract Labor Standards
52.222-50	Combating Trafficking in Persons
52.222-55	Minimum Wages for Contractor Workers Under Executive Order 14026
52.222-62	Paid Sick Leave Under Executive Order
52.223-6	Drug-Free Workplace (applicable only to US subs exceeding $150,000 not applicable to purchases of commercial items at any amount)
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING
52.225-13	Restrictions on Certain Foreign Purchases
52.227-1	Authorization and Consent (applicable only to US subs exceeding $150,000)
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement (applicable only to US subs exceeding $150,000)
52.227-3	Patent Indemnity (applicable only to US subcontractors/vendors)
52.227-9	Refund of Royalties
52.228-3	Workers' Compensation Insurance (Defense Base Act) (applicable only to US subcontractors/vendors)
52.228-4	Workers' Compensation and War-Hazard Insurance Overseas
52.228-9	Cargo Insurance (applicable only when procuring goods that will be transported)
52.232-1	Payments
52.232-25	Prompt Payment
52.232-34	Payment by Electronic Funds Transfer-Other than System for Award Management
52.232-39	Unenforceability of Unauthorized Obligations
52.232-40	Providing Accelerated Payments to Small Business Subcontractors
52.233-1	Disputes

52.233-4	Applicable Law for Breach of Contract Claim
52.243-1	Changes – Fixed Price
52.246-23	INSPECTION OF SERVICES FIXED-PRICE
52.246-23	Limitation of Liability (applicable only if purchasing an item valued under $150,000)
52.246-24	Limitation of Liability – High-Value Items (only if purchasing an item exceeding $150,000)
52.246-25	Limitation of Liability - Services (applicable only for services)
52.247-63	Preference for U.S. Air Flag Carriers (applicable only when international travel will occur)
52.249-4	Termination for Convenience of the Government (Services)(Short-Form)

AIDAR

752.202-1	Definitions, Alternate 70 USAID Definitions Clause - General Supplement for Use in All USAID Contracts & Alternate 72 USAID Definitions Clause - Supplement for USAID Contracts Involving Performance Overseas
752.209-71	Organizational Conflicts of Interest Discovered After Award
752.211-70	Language and Measurement
752.222-70	USAID Disability Policy
752.225-70	Source and Nationality Requirements
752.228-3	Workers Compensation Insurance (Defense Base Act)
752.228-7	Insurance -- Liability to Third Persons
752.228-9	Cargo Insurance (applicable only when procuring goods that will be transported)
752.228-70	Medical Evacuation (MEDEVAC)
752.245-70	Government Property-USAID Reporting Requirements (applicable only when subcontractor/vendor required to procure non-expendable property)
752.245-71	Title to and Care of Property (applicable only when sub required to procure non-expendable property)
752.7009	Marking (Jan 1993)
752.7025	Approvals (Apr 1984)
752.7027	Personnel (Dec 1990)

752.7032	International Travel Approval and Notification Requirements (applicable only when international travel is authorized)
752.7033	Physical Fitness (applicable only to International Subcontractor/vendor when International travel is authorized)
752.7034	Acknowledgement and Disclaimer (applicable only for the purchase of publications, videos, or other information/media products)
752.7035	Public Notices (Dec 1991)
752.7036	USAID IMPLEMENTING PARTNER NOTICES (IPN) PORTAL FOR ACQUISITION
752.7037	CHILD SAFEGUARDING STANDARDS
752.7038	NONDISCRIMINATION AGAINST END-USERS OF SUPPLIES AND SERVICES

[End of Section I]

PART III – LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

Section J and its contents here within are only applicable to the USAID portion of funding.

J. LIST OF ATTACHMENTS

J.1 Representations, Certifications and Other Statements of Offerors

Cadmus Reps and Certs ($10K+).doc

J.2 Budget Template

Budget Template.xlsx

J.3 Responses to Questions from Offerors

Section J.3 Responses to Questio

J.4 Responses to 2nd Round of Questions from Offerors

Section J.4 Responses to 2nd Rou

PART IV – REPRESENTATIONS AND INSTRUCTIONS

K. REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR RESPONDENTS

See attachment under Section J.1.

[End of Section K]

L. INTSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS

Proposals are due in electronic copy only, in MS Word, MS Excel, and/or PDF formats, by **November 8, 2024** at 5:00 PM EDT time. Tables or charts in MS Excel format should be labeled appropriately. The email must not exceed 5MB in size. Technical and price proposals need to be submitted in separate electronic files and emailed to insert email.

Technical proposals shall consist of no more than twenty (20) pages and include details of the approach, timelines for completion of the project, a summary of qualifications of key personnel who would be assigned to the project, and necessary contact information. Additional tables, technical instructions, and CVs of key personnel, not to exceed two pages in length each, should be included in an appendix to the technical proposal and will not count towards the 20-page limit (margins should be 1 inch on each side, text should be single spaced, and font should be no less than 11 point). A separate financial proposal shall be provided. No cost information shall be provided in the technical proposal. Detailed specifications of the technical and financial proposals are shown below. **Offerors must submit a financial proposal along with their technical approach, which should be in a separate Microsoft Excel file.**

Your proposal shall be accompanied by a letter of transmittal prepared on your company letterhead stationery and signed by an individual authorized to commit the company to the proposal. The cover letter shall identify the following as well as all enclosures being transmitted as part of the proposal:

- The name, and address, of your company
- RFP number
- Point of Contact name, title, telephone number, and email address
- Unique Entity Identifier (UEI)
- Acknowledgement that it transmits an offer in response to the RFP that is valid for a minimum of 60 days from the proposal due date.

L.1 Technical/Methodical Approach

Offerors must describe their overall technical approach and methodology to be utilized by the Offeror for the design, development, implementation, and achievement of the stated Tasks and Deliverables provided in the RFP. The Offeror shall articulate how it intends to address each of the required tasks as well as desired system functionalities, features and project deliverables listed, in addition to any suggestions and recommendations to these areas while demonstrating the project management approach and framework to be utilized.

When evaluating the **Technical Approach**, Technical Evaluation Committee (TEC) are to consider the requirements from the RFP and to note in their comments whether Offeror demonstrated it satisfies these points:

- **Extent to which the Offeror demonstrates an understanding of the development context and Statement of Work Comprehensiveness of proposed approach.**
- **Clarity and appropriateness of proposed activity.**
- **Realistic Implementation plan and include all proposed elements of activity.**
- **Offeror to propose well-determined and effective approaches and solutions to achieve the tasks.**

L.2 Personnel/Staffing

The proposal must identify, in summary format of 2-3 sentences, the names, anticipated positions of the field team leaders, and essential personnel proposed to perform the requirements of this scope of work, tasks, and deliverables. The narrative shall include the percentage of staff time of principals and managers on this activity.

The approach should include the organizational structure of the entire project team and explain how the staffing plan will result in successful implementation of the proposed technical approach and accomplish the objectives of the activity. If the Offeror anticipates using any sub-awards, include the roles and responsibilities of each sub-awardee and the lines of authority and communication.

CVs (not to exceed two pages each) that clearly describe education, experience and professional credentials, and biodata forms shall be completed and attached for the proposed personnel and submitted to Annex. These pages do not count towards the page limitation for this section.

When evaluating Personnel/Staffing, TEC to consider the requirements from the RFP and indicate **the quality and appropriateness of the proposed personnel, including the extent to which they meet qualification requirements and convincingly demonstrate the Offeror's ability to effectively and successfully achieve the contract's objectives.**

L.3 Past Performance/References

Proposal description on how the past performance of the Offeror and its team (including all partners of a coalition/joint venture) is relevant to performance of the Contract. The Offeror shall submit a list (up to five) of current and past similar work and assignments completed in the past five years that were similar in size, scope, and complexity.

Offerors must provide a past performance annex with the following information: Name of Project, Period of Performance, Total Estimated Cost, Geographic Location of Implementation, Summary of what the project was, Name of Client/Funder, Point of Contact Name, Phone Number, and Email.

The past performance annex will not count against the page limit.

When evaluating Past Performance/References, TEC to consider the requirements from the RFP and the Offeror's overall, previous successful experience implementing similar activities, including:

- **Timeliness;**
- **Technical Expertise and Capability;**
- **Communication and Collaboration;**
- **Compliance with USAID Regulations (if applicable);**
- **Quality of work;**
- **Problem-solving and flexibility;**
- **Staffing and personnel management;**
- **Financial management and budget compliance;**
- **Cultural sensitivity and local engagement; and**

- **Risk management.**

Cadmus reserves the right to seek additional sources of past performance as it sees fit in order to conduct a comprehensive evaluation of an offeror.

L.4 Capability Statement

Must explain Offeror's understanding of desired system and requirements as well as its capability to perform the scope of work, tasks, and deliverables. Offeror shall demonstrate it has the necessary organizational systems and procedures, e.g., personnel policies, travel policies, project management, equipment, supplies, and personnel in place to successfully comply with contract requirements and accomplish expected results.

Scores must be based on the extent to which the Offeror and its partners or subcontractors (if any) convincingly demonstrate its institutional capability to effectively and successfully achieve the objectives in the statement of work and implement its proposed technical approach. When evaluating the Capability Statement, TEC to consider the requirements from the RFP and to note in their comments whether Offeror demonstrated it satisfies these points:

- **Organizational competence relative to the Tasks and Deliverables, including knowledge of and at least 7 years' experience working infeasibility studies area;**
- **Capabilities mobilizing short-term technical assistance experts and teams**

L.5 Cost Proposal

Offerors will be required to submit a cost estimate for services, a cost estimate by major cost categories/line items, and cost summary.

Using the table below, Offerors must provide a cost estimate for each milestone/deliverable.

Milestone/Deliverable	Payment Amount	Payer	Due Date*
Rapid Analysis (desk research and key stakeholder interviews) and Madagascar Deep Dive	$		March 31, 2025
Draft Report	$		April 30, 2025
Stakeholder feedback sessions (and accompanying slide deck)	$		May 30, 2025
Final Report including Madagascar deep dive as a section and also as a standalone report and Policy Dialogue (and accompanying slide deck)	$		June 30, 2025
TOTAL	$		

Using the budget template at Section J.2, Offerors are required to provide a cost estimate for major cost categories/line items (e.g. labor, materials, equipment, ODCs) without breaking down each category in great detail.

Offerors are required to provide a cost summary narrative that must provide sufficient detail to support how the Offeror arrived at the fixed price proposed.

[End of Section L]

M. EVALUATION FACTOR FOR AWARD

M.1 General Information

Proposals will be evaluated in accordance with Section M of this RFP. An award will be given to the responsible offeror whose proposal offers the best value, considering both cost and non-cost factors.

The submitted technical information will be scored by a technical evaluation committee using the technical criteria shown below. The evaluation committee may include individuals who are not employed by Cadmus.

The following are the evaluation criteria for this RFP:

Criterion	Maximum Points
Technical/Methodical approach (see L.1)	35
Personnel/Staffing (see L.2)	30
Past Performance/References (see L.3)	15
Capability Statement (see L.4)	10
Cost (see L.5)	10
Total points	**100**

M.2 Technical Evaluation Factors

Criterion	Maximum Points
Technical/Methodical approach (see L.1)	35
Personnel/Staffing (see L.2)	30
Past Performance/References (see L.3)	15
Capability Statement (see L.4)	10
Total points	**90**

M3. Cost Evaluation (see L.5)

Cost will be evaluated and assigned a rating of **10 points**.

Cadmus will assess whether the proposed price is fair and reasonable. Meaning is the price in alignment with market rates and justifiable for the scope of work deliverables.

Cadmus reserves the right to request additional information if it is necessary to better understand the basis of the proposed price to verify that it is reasonable. Cadmus reserves the right to evaluate price realism if there are concerns that the price proposed is too low to meet the contract requirements.

M.4 Source Selection/Best Value

Cadmus and BMZ intend to award contracts resulting from this solicitation to the responsible Offeror whose proposal represents the best value after evaluation in accordance with the factors as set forth in this solicitation. Cadmus and BMZ will award contracts to the Offeror whose proposal represents the best value. An award to a higher priced Offeror could be made if a determination is made that the higher technical evaluation of that Offeror merits the additional cost/price, and therefore represents the best value.

Price will be evaluated for reasonableness. Offerors are encouraged to discount their rates. If price discounts are offered, identify the percentage of price discount and/or price reduction offered. Offerors should ensure that their initial proposal constitutes their best offer in terms of both price and the technical solution being proposed.

[End of Section M]