ANNEX B: USAID CONTRACT CLAUSES

Part I - Flow-down Clauses from USAID/*Kenya and East Africa Evaluation, Assessments, and Analyses (EAA)* IDIQ Contract # *72062320D00001*

SECTION D – PACKAGING AND MARKING

D.1 AIDAR 752.7009 – MARKING (JAN 1993)

(a) It is USAID policy that USAID-financed commodities and shipping containers, and project construction sites and other project locations be suitably marked with the USAID emblem. Shipping containers are also to be marked with the last five digits of the USAID financing document number. As a general rule, marking is not required for raw materials shipped in bulk (such as coal, grain, etc.), or for semi-finished products which are not packaged.

(b) Specific guidance on marking requirements should be obtained prior to procurement of commodities to be shipped, and as early as possible for project construction sites and other project locations. This guidance will be provided through the cognizant technical office indicated on the cover page of this Contract, or by the Mission Director in the Cooperating Country to which commodities are being shipped, or in which the project site is located.

(c) Authority to waive marking requirements is vested with the Regional Assistant Administrators, and with Mission Directors.

(d) A copy of any specific marking instructions or waivers from marking requirements is to be sent to the Contracting Officer; the original should be retained by the Contractor.

D.2 BRANDING POLICY

The Contractor will comply with the requirements of the policy directives and required procedures outlined in USAID Automated Directive System (ADS) 320.3.2 "Branding and Marking in USAID Direct Contracting" (version from January 8, 2007) at https://www.usaid.gov/sites/default/files/documents/1868/320.pdf; and USAID "Graphic Standards Manual" available at www.usaid.gov/branding, or any successor branding policy.

As per 320.3.2 Branding and Marking in USAID Direct Contracts, USAID policy is to require exclusive branding and marking in USAID direct acquisitions. "Exclusive Branding" means that the program is positioned as USAID's, as showcased by the program name (e.g., "The USAID/EAA Program"). "Exclusive Marking" means Contractors may only mark USAID-funded programs, projects, activities, public communications, and commodities with the USAID Standard Graphic Identity and, where applicable, the host-country government or ministry symbol or another U.S. Government logo. It is USAID's policy that Contractors' and Subcontractors' corporate identities or logos must not be used on USAID-funded program materials.

D.3 BRANDING STRATEGY AND MARKING PLAN

Approved Branding Implementing Plan and Marking Plan are incorporated as Attachment J.2.

[END OF SECTION D]

SECTION E – INSPECTION AND ACCEPTANCE

E.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following Contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this Contract. See https://acquisition.gov/browse/index/far for electronic access to the full text of a FAR clause.

NUMBER	TITLE *FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)*	DATE
52.246-4	INSPECTION OF SERVICES – FIXED PRICE	AUG 1996
52.246-5	INSPECTION OF SERVICES – COST REIMBURSEMENT	APR 1984

[END OF SECTION E]

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 AAPD 16-02 – RESTRICTIONS AGAINST DISCLOSURE (MAY 2016)

(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.

H.2 AAPD 16-02 – MEDIA AND INFORMATION HANDLING AND PROTECTION (APRIL 2018)

(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; 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 "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. Within 45 calendar days of the award, 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).

H.3 AAPD 16-02 – SKILLS AND CERTIFICATION REQUIREMENTS FOR PRIVACY AND SECURITY STAFF (APRIL 2018)

(a) Applicability: This special Contract requirements applies to the Contractor, its subcontractors and personnel providing support under this Contract and addresses the Privacy Act of 1974 (5 U.S.C. 552a - the Act), the Federal Information Security Management Act (FISMA) of 2002 (FISMA, Public Law 107-347. 44 U.S.C. 3531-3536, as amended).

(b) Contractor employees filling the role of Information System Security Officer and Information Security Specialists must possess a Certified Information Systems Security Professional (CISSP) certification at the time of Contract award and maintain their certification throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor employees must provide proof of their certification status upon request.

(c) Contractor employees filling the role of Privacy Analysts must possess a Certified Information Privacy Professional (CIPP) credential with either a CIPP/US or a CIPP/G at the time of the Contract award and must maintain the credential throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor employees must provide proof of their certification status upon request.

H.4 AAPD 16-02 – SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APRIL 2018)

(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 IT cybersecurity requirements as well as current Federal regulations and guidance found in the Federal Information Security Management Act (FISMA), Privacy Act of 1974, E-Government Act of 2002, Section 208, 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.

H.5 AAPD 16-02 – CLOUD COMPUTING (APRIL 2018)

(a) Definitions. As used in this special Contract requirement:

"Access" means the ability or opportunity to gain knowledge of Government or Government-related data or any other data collected or maintained on behalf of the United States Government under this Contract.

"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.

"Government data" means any information, document, media, or machine-readable material, regardless of physical form or characteristics, which is created or obtained in the course of official Government business.

"Government-related data" means any information, document, media, or machine-readable material, regardless of physical form or characteristics, which is created or obtained by a Contractor through the storage, processing, or communication of Government data. This does not include a Contractor's business records, e.g., financial records, legal records, or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

"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.

"Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

(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, government data and Government-related data.

(1) The Contractor shall not access, use, or disclose Government data 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, Government data 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 Government data only to manage the operational environment that supports the government data 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, National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Government data and Government-related data, 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, e-Records and legal or security investigations.

(3) The Contractor shall retain and maintain all Government data 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 Government data and Government-related data 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 Government data: The Contractor shall notify the Government immediately of any requests from a third party for access to Government data or Government-related data, 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 Government data to a third party. The Contractor shall cooperate with the Government to take all measures to protect Government data 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: CIO-HELPDESK@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 Government information. The CSP does not have rights to the USAID information for any purposes other than those explicitly stated in the Contract.

(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, 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 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 Government 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 a provisional 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 non-criminal 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.

H.6 USAID-FINANCED THIRD-PARTY WEB SITES (NOV 2017)

(a) Definitions:

"Third-party web sites"

Sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of a Contract. Third-party Web sites include project sites.

(b) The Contractor must adhere to the following requirements when developing, launching, and maintaining a third-party Web site funded by USAID for the purpose of meeting the project implementation goals:

(1) Prior to Web site development, the Contractor must provide information as required in Section C-Statement of Work of the Contract (including a copy of the Contractor's privacy policy) to the Contracting Officer's Representative (COR) for USAID's Bureau for Legislative and Public Affairs (LPA) evaluation and approval. The Contractor must notify the COR of the Web site URL as far in advance of the site's launch as possible and must not launch the Web site until USAID's (LPA) approval has been provided through the COR. The Contractor must provide the COR with any changes to the privacy policy for the duration of the Contract.

(2) The Contractor must collect only the amount of information necessary to complete the specific business need as required by statute, regulation, or Executive Order.

(3) The Contractor must comply with Agency branding and marking requirements comprised of the USAID logo and brandmark with the tagline "from the American people," located on the USAID Web site at www.usaid.gov/branding, and USAID Graphics Standards manual at http://www.usaid.gov.

(4) The Web site must be marked on the index page of the site and every major entry point to the Web site with a disclaimer that states: "The information provided on this Web site is not official U.S. Government information and does not represent the views or positions of the U.S. Agency for International Development or the U.S. Government."

(5) The Web site must provide persons with disabilities access to information that is comparable to the access available to others. As such, all site content must be compliant with the requirements of the Section 508 amendments to the Rehabilitation Act.

(6) The Contractor must identify and provide to the COR, in writing, the contact information for the information security point of contact. The Contractor is responsible for updating the contact information whenever there is a change in personnel assigned to this role.

(7) The Contractor must provide adequate protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted on the Web sites. To minimize security risks and ensure the integrity and availability of information, the Contractor must use sound: system/software management; engineering and development; and secure coding practices consistent with USAID standards and information security best practices. Rigorous security safeguards, including but not limited to, virus protection; network intrusion detection and prevention programs; and vulnerability management systems must be implemented, and critical security issues must be resolved as quickly as possible or within 30 days. Contact the USAID Chief Information Security Officer (CISO) at ISSO@usaid.gov for specific standards and guidance.

(8) The Contractor must conduct periodic vulnerability scans, mitigate all security risks identified during such scans, and report subsequent remediation actions to CISO at ISSO@usaid.gov and COR within 30 workdays from the date vulnerabilities are identified. The report must include

disclosure of the tools used to conduct the scans. Alternatively, the Contractor may authorize USAID CISO at ISSO@usaid.gov to conduct periodic vulnerability scans via its Web-scanning program. The sole purpose of USAID scanning will be to minimize security risks. The Contractor will be responsible for taking the necessary remediation action and reporting to USAID as specified above.

(c) For general information, agency graphics, metadata, privacy policy, and Section 508 compliance requirements, refer to http://www.usaid.gov.

H.7 SUBMISSION OF DATASETS TO THE DEVELOPMENT DATA LIBRARY (DDL) (OCT 2014)

(a) Definitions. For the purpose of submissions to the DDL:

(1) "Dataset" is an organized collection of structured data, including data contained in spreadsheets, whether presented in tabular or non-tabular form. For example, a Dataset may represent a single spreadsheet, an extensible mark-up language (XML) file, a geospatial data file, or an organized collection of these. This requirement does not apply to aggregated performance reporting data that the Contractor submits directly to a USAID portfolio management system or to unstructured data, such as email messages, PDF files, PowerPoint presentations, word processing documents, photos and graphic images, audio files, collaboration software, and instant messages. Neither does the requirement apply to the Contractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information. Datasets submitted to the DDL will generally be those generated with USAID resources and created in support of Intellectual Work that is uploaded to the Development Experience Clearinghouse (DEC) (see AIDAR 752.7005 "Submission Requirements for Development Experience Documents")

(2) "Intellectual Work" includes all works that document the implementation, monitoring, evaluation, and results of international development assistance activities developed or acquired under this award, which may include program and communications materials, evaluations and assessments, information products, research and technical reports, progress and performance reports required under this award (excluding administrative financial information), and other reports, articles and papers prepared by the Contractor under the award, whether published or not. The term does not include the Contractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information.

(b) Submissions to the Development Data Library (DDL)

(1) The Contractor must submit to the Development Data Library (DDL), at www.usaid.gov/data, in a machine-readable, non-proprietary format, a copy of any Dataset created or obtained in performance of this award, including Datasets produced by a subcontractor at any tier. The submission must include supporting documentation describing the Dataset, such as code books, data dictionaries, data gathering tools, notes on data quality, and explanations of redactions.

(2) Unless otherwise directed by the Contracting Officer (CO) or the Contracting Officer Representative (COR), the Contractor must submit the Dataset and supporting documentation within thirty (30) calendar days after the Dataset is first used to produce an Intellectual Work or is of sufficient quality to produce an Intellectual Work. Within thirty (30) calendar days after award completion, the Contractor must submit to the DDL any Datasets and supporting documentation that have not previously been submitted to the DDL, along with an index of all Datasets and

Intellectual Work created or obtained under the award. The Contractor must also provide to the COR an itemized list of any and all DDL submissions.

The Contractor is not required to submit the data to the DDL, when, in accordance with the terms and conditions of this award, Datasets containing results of federally funded scientific research are submitted to a publicly accessible research database. However, the Contractor must submit a notice to the DDL by following the instructions at www.usaid.gov/data, with a copy to the COR, providing details on where and how to access the data. The direct results of federally funded scientific research must be reported no later than when the data are ready to be submitted to a peer-reviewed journal for publication, or no later than five calendar days prior to the conclusion of the award, whichever occurs earlier.

(3) The Contractor must submit the Datasets following the submission instructions and acceptable formats found at www.usaid.gov/data.

(4) The Contractor must ensure that any Dataset submitted to the DDL does not contain any proprietary or personally identifiable information, such as social security numbers, home addresses, and dates of birth. Such information must be removed prior to submission.

(5) The Contractor must not submit classified data to the DDL.

H.8 ORGANIZATIONAL CONFLICTS OF INTEREST: PRECLUSION FROM FURNISHING CERTAIN SERVICES AND RESTRICTION ON USE OF INFORMATION (SEP 2018)

(a) Task Orders under this Contract may require the Contractor to furnish important services in support of evaluation of Contractors or of specific activities. In accordance with the principles of FAR Subpart 9.5 and USAID policy, the Contractor will be ineligible to furnish, as a Prime or Subcontractor or otherwise, implementation services under any Contract or Task Order that results in response to findings, proposals, or recommendations in an evaluation report written by the Contractor. This preclusion will apply to any such awards made within 18 months of USAID accepting the report, unless the Head of the Contracting Activity authorizes a waiver (in accordance FAR 9.503) determining that preclusion of the Contractor from the implementation work would not be in the Government's interest.

(b) In addition, by accepting this Contract, the Contractor agrees that it will not use or make available any information obtained about another organization under the Contract in the preparation of proposals or other documents in response to any solicitation for a Contract or Task Order.

(c) If the Contractor gains access to proprietary information of other company(ies) in performing this evaluation, the Contractor must agree with the other company(ies) to protect their information from unauthorized use or disclosure for as long as it remains proprietary and must refrain from using the information for any purpose other than that for which it was furnished. The Contractor must provide a properly executed copy of all such agreements to the CO.

H.9 AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this Contract is **935** unless specified otherwise in Task Orders.

H.10 AIDAR 752.231-72 – CONFERENCE PLANNING AND REQUIRED APPROVALS (AUG 2013)

(a) Definitions. Conference means a seminar, meeting, retreat, symposium, workshop, training activity or other such event that requires temporary duty travel of USAID employees. For the purpose of this policy, an employee is defined as a U.S. direct hire; personal services Contractor, including U.S. PSCs, Foreign Service National (FSN)/Cooperating Country National (CCN) and Third Country National (TCN); or a Federal employee detailed to USAID from another government agency.

(b) The Contractor must obtain approval from the Contracting Officer or the contracting officer's representative (COR), if delegated in the Contracting Officer's Representative Designation Letter, as prescribed in 731.205-43, prior to committing costs related to conferences funded in whole or in part with USAID funds when:

(1) Twenty (20) or more USAID employees are expected to attend.

(2) The net conference expense funded by USAID will exceed $100,000 (excluding salary of employees), regardless of the number of USAID participants.

(c) Conferences approved at the time of award will be incorporated into the award. Any subsequent requests for approval of conferences must be submitted by the Contractor to the USAID Contracting Officer Representative (COR). The Contracting Officer representative will obtain the required agency approvals and communicate such approvals to the Contractor in writing.

(d) The request for conference approval must include:

(1) A brief summary of the proposed event;

(2) A justification for the conference and alternatives considered, e.g., teleconferencing and videoconferencing;

(3) The estimated budget by line item (e.g., travel and per diem, venue, facilitators, meals, equipment, printing, access fees, ground transportation);

(4) A list of USAID employees attending and a justification for each; and the number of other USAID-funded participants (e.g., Institutional Contractors);

(5) The venues considered (including government-owned facility), cost comparison, and justification for venue selected if it is not the lowest cost option;

(6) If meals will be provided to local employees (a local employee would not be in travel status), a determination that the meals are a necessary expense for achieving Agency objectives; and

(7) A certification that strict fiscal responsibility has been exercised in making decisions regarding conference expenditures, the proposed costs are comprehensive and represent the greatest cost

advantage to the U.S. Government, and that the proposed conference representation has been limited to the minimum number of attendees necessary to support the Agency's mission.

H.11 DISCLOSURE OF INFORMATION

(a) Contractors are reminded that information furnished under this solicitation may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not necessarily preclude disclosure when the U.S. Office of Personnel Management (OPM or The Government) determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

(b) Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this Contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract.

(c) In performance of this Contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees.

(d) Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 19 U.S.C. 641. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine of up to $10,000, or imprisoned up to ten years, or both.

H.12 ENVIRONMENTAL COMPLIANCE

1)

a) Section 117 of the Foreign Assistance Act of 1961, as amended, requires that the impact of USAID's activities on the environment be considered and that USAID include environmental sustainability as a central consideration in designing and carrying out its development programs. This mandate is codified in Federal Regulations (22 CFR 216) and in USAID's Automated Directives System (ADS) Parts 201.5.10g and 204 (http://www.usaid.gov/policy/ads/200/), which, in part, require that the potential environmental impacts of USAID-financed activities are identified prior to a final decision to proceed and that appropriate environmental safeguards are adopted for all activities.

b) In addition, the Contractor must comply with host country environmental regulations unless otherwise directed in writing by USAID. In case of conflict between host country and USAID regulations, the latter shall govern.

2) An Initial Environmental Examination (IEE) for this Activity has been approved by the Bureau Environmental Office.

- The IEE concludes that, Negative Determinations with Conditions is recommended for this activity per 22 CFR 216.3 (a)(2)(iii), and Request for Categorical Exclusions (RCE) is recommended for this activity per 22 CFR §216.2 (c)(2)(i) and (iii) for or analyses, studies, academic or research workshops and meetings; Per 22 CFR §216.2 (c)(2)(v) for activities involving document and information transfers.

- As required by ADS 204.3.4, USAID will "actively monitor ongoing activities for compliance with approved recommendations and modify or end activities that are not in compliance" and ensure that adequate time and resources are available to bring this activity into compliance with the requirements of this IEE. If during implementation, this activity is considered outside the above framework as described in the subject categorical exclusion, and that it may directly affect the environment, an IEE or amended RCE shall be submitted, as appropriate.

3) USAID anticipates that environmental compliance and achieving optimal development outcomes for the proposed activities will require environmental management expertise.

H.13 EXECUTIVE ORDER ON TERRORISM FINANCING

The Contractor is reminded that U.S. Executive Orders (including E.O. 13224) and U.S. law prohibit transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. FAR 25.701 prohibits agencies and their Contractors and subcontractors from acquiring any supplies or services from individuals or organizations, if any proclamation, Executive Order, Office of Foreign Assets Control (OFAC) regulations, or statute administered by OFAC would prohibit such a transaction. Accordingly, the Contracting Officer must check the U.S. Department of the Treasury's OFAC List to ensure that the names of the Contractor and proposed subcontractors (and individuals from those organizations who have been made known to them), are not on the list. Mandatory FAR clause 52.225-13 Restrictions on Certain Foreign Purchases is included by reference in Section I.1 of this Contract. By accepting this Contract, the Contractor acknowledges and agrees that it is aware of the list as part of its compliance with the requirements of that clause.

H.14 FOREIGN GOVERNMENT DELEGATIONS TO INTERNATIONAL CONFERENCES (JAN 2002)

Funds in this Contract may not be used to finance the travel, per diem, hotel expenses, meals, conference fees or other conference costs for any member of a foreign government's delegation to an international conference sponsored by a public international organization, except as provided in ADS Mandatory Reference "Guidance on Funding Foreign Government Delegations to International Conferences" [https://www.usaid.gov/sites/default/files/documents/1868/350maa.pdf] or as approved by the Contracting Officer's Representative (COR).

H.15 GENDER CONSIDERATION

To the greatest extent possible, the Contractor must seek to include both men and women in all aspects of this program including participation and leadership in (e.g., meetings, training, etc.).

The Contractor must collect, analyze and submit to USAID sex-disaggregated data and proposed actions that will address any identified gender-related issues. Further requirements on this are included in Section C.

USAID policy requires that gender issues be addressed as appropriate in all USAID-funded activities. The technical approach must describe how gender considerations will be integrated throughout the program

and into specific activities as appropriate. The Contractor must look for gender implications or opportunities in the program, seeking to address embedded gender issues and promote gender equity, as appropriate, in all phases of program implementation and internal management. This program must address gender concerns in a fundamental way –simply setting aside funds for training of female council members, for example, will not alone be considered sufficient. Specific activities for women are appropriate. Gender indicators must be defined and tracked by the Contractor and the Contractor will complete an analysis of gender as part of its initial stages of implementation.

H.16 GOVERNMENT FURNISHED FACILITIES OR PROPERTY

The Contractor and any employee or consultant of the Contractor is prohibited from using U.S. Government facilities (such as office space or equipment) or U.S. Government clerical or technical personnel in the performance of the services specified in the Contract unless the use of Government facilities or personnel is specifically authorized in the Contract or is authorized in advance, in writing, by the COR.

H.17 INSURANCE AND SERVICES

FAR 52.228-3 – WORKERS' COMPENSATION INSURANCE (DEFENSE BASE ACT) (JUL 2014)

(a) The Contractor shall:

(1) Before commencing performance under this Contract, establish provisions to provide for the payment of disability compensation and medical benefits to covered employees and death benefits to their eligible survivors, by purchasing workers' compensation insurance or qualifying as a self-insurer under the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 932) as extended by the Defense Base Act (42 U.S.C. 1651, et seq.), and continue to maintain provisions to provide such Defense Base Act benefits until Contract performance is completed;

(2) Within ten days of an employee's injury or death or from the date the Contractor has knowledge of the injury or death, submit Form LS-202 (Employee's First Report of Injury or Occupational Illness) to the Department of Labor in accordance with the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 930(a), 20 CFR 702.201 to 702.203);

(3) Pay all compensation due for disability or death within the time frames required by the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 914, 20 CFR 702.231 and 703.232);

(4) Provide for medical care as required by the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 907, 20 CFR 702.402 and 702.419);

(5) If controverting the right to compensation, submit Form LS-207 (Notice of Controversion of Right to Compensation) to the Department of Labor in accordance with the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 914(d), 20 CFR 702.251);

(6) Immediately upon making the first payment of compensation in any case, submit Form LS-206 (Payment of Compensation Without Award) to the Department of Labor in

accordance with the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 914(c), 20 CFR 702.234);

(7) When payments are suspended or when making the final payment, submit Form LS-208 (Notice of Final Payment or Suspension of Compensation Payments) to the Department of Labor in accordance with the Longshore and Harbor Workers' Compensation Act (33 U.S.C. 914 (c) and (g), 20 CFR 702.234 and 702.235); and

(8) Adhere to all other provisions of the Longshore and Harbor Workers' Compensation Act as extended by the Defense Base Act, and Department of Labor regulations at 20 CFR Parts 701 to 704.

(b) For additional information on the Longshore and Harbor Workers' Compensation Act requirements see http://www.dol.gov/owcp/dlhwc/lsdba.htm.

(c) The Contractor shall insert the substance of this clause including this paragraph (c), in all subcontracts to which the Defense Base Act applies.

AIDAR 752.228-3 – WORKER'S COMPENSATION INSURANCE (DEFENSE BASE ACT) (DEC 1991)

(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.

(b) If USAID or the Contractor has secured a waiver of DBA coverage (see 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 a like requirement to provide overseas workmen's compensation insurance coverage and obtain DBA coverage under the USAID requirements Contract.

(d) Allied World Assurance Company is the only insurance underwriter authorized to write DBA insurance under USAID Contracts. To obtain DBA insurance, Contractors are to contact Allied's agent, Aon Risk Insurance Services West, Inc. at:

(1) 199 Fremont St., Suite 1400
San Francisco, CA 94105

Primary Contact: Fred Robinson; Phone: (415) 486-7516; Email: Fred.Robinson@aon.com
Secondary Contact: Angela Falcone; Phone: (415) 486-7000; Email: Angela.Falcone@aon.com

OR

(2) 1120 20th St., N.W., Suite 600

Washington D.C. 20036

Primary Contact: Ellen Rowan; Phone: (202) 862-5306; Email: Ellen.Rowan@aon.com
Secondary Contact: Chris Thompson; Phone: (202) 862-5302; Email: Chris.Thompson@aon.com

(e) The Contractor shall be entitled to be reimbursed for the cost of insurance provided to its employees pursuant to the Contract clause at FAR 52.228-3, "Workers' Compensation Insurance (Defense Base Act)," at the USAID authorized rate (Please refer to latest AAPD) of employee remuneration. The Contractor is herein notified that DBA insurance coverage is a requirement for all Prime Contractor employees and subcontractor employees under this Contract pursuant to FAR 52.228-3. DBA-covered employees are also entitled to benefits under the War Hazards Compensation Fund. As this is a U.S. Government established fund and its benefits are provided at no additional cost to the Contractor above the cost of DBA insurance, the Contractor is not entitled to reimbursement for War Hazards Compensation Fund coverage. If the Contractor provides additional accidental death and disability or life insurance to its employees, the cost of the additional insurance will be considered a fringe benefit and will be allowable as provided by FAR 31.205-6(m).

H.18 LANGUAGE REQUIREMENTS

All deliverables must be produced in English.

H.19 LOGISTIC SUPPORT

The Contractor shall be responsible for furnishing all logistic support in the United States and overseas.

H.20 STANDARDS OF CONDUCT – IMPROPER BUSINESS PRACTICES

Corruption or any other improper business practices related to this solicitation and any resulting Contract(s) will not be tolerated. Transactions relating to the expenditure of public funds require the highest degree of public trust and an impeccable standard of conduct by Contractors, subcontractors and any other agent acting in connection with this Contract. Examples of such unacceptable behavior include but are not limited to providing or offering of bribes to any person associated with the Contract or any subcontracts; soliciting or accepting kickbacks or bribes; and knowingly making any false or misleading accounting reports or financial statements. Contractors, subcontractors and any other agents acting under Contracts awarded herein are expected to employ due diligence and have internal controls in place towards practicing good governance in execution of the Contract. Any one of these entities found to have engaged in illegal activity, improper behavior, or corrupt practices will be subject to corrective actions in accordance with the respective FAR clause incorporated into this solicitation and any resulting Contract(s).

H.21 USAID DISABILITY POLICY – ACQUISITION (DEC 2004)

(a) The objectives of the USAID Disability Policy are (1) to enhance the attainment of United States foreign assistance program goals by promoting the participation and equalization of opportunities of individuals with disabilities in USAID policy, country and sector strategies, activity designs and implementation; (2) to increase awareness of issues of people with disabilities both within USAID programs and in host countries; (3) to engage other U.S. government agencies, host country counterparts, governments, implementing organizations and other donors in fostering a climate of

nondiscrimination against people with disabilities; and (4) to support international advocacy for people with disabilities. The full text of the policy paper can be found at the following website: https://pdf.usaid.gov/pdf_docs/PDABQ631.pdf.

(b) USAID therefore requires that the Contractor not discriminate against people with disabilities in the implementation of USAID programs and that it makes every effort to comply with the objectives of the USAID Disability Policy in performing this Contract. To that end and within the scope of the Contract, the Contractor's actions must demonstrate a comprehensive and consistent approach for including men, women and children with disabilities.

H.22 FOREIGN TAXES AND DUTIES

Foreign taxes and duties are an allowable expense under this IDIQ in accordance with FAR regulations. Contractors may be reimbursed for the cost of taxes and duties incurred if allowable and allocable to the work performed. USAID missions may have specific Value Added Tax (VAT) and duty reimbursement or exception procedures in place that will be communicated at the Task Order level. Contractors must follow these procedures as it may impact the allowability of incurred VAT and/or duty costs.

[END OF SECTION H]

PART II – CONTRACT CLAUSES

SECTION I – CONTRACT CLAUSES

I.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

As applicable, the following Contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date), as applicable, in accordance with the clause at FAR 52.252-2 "CLAUSES INCORPORATED BY REFERENCE" in this section of the Contract. See https://acquisition.gov/browse/index/far for electronic access to the full text of a FAR clause.

NUMBER	TITLE	DATE
FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)		
52.202-1	DEFINITIONS	NOV 2013
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	MAY 2014
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	SEP 2006
52.203-7	ANTI-KICKBACK PROCEDURES	MAY 2014
52.203-8	CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	OCT 2010
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	OCT 2015
52.203-16	PREVENTING PERSONAL CONFLICTS OF INTEREST	DEC 2011
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND	

	REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS – REPRESENTATION	JAN 2017
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNA CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER	MAY 2011
52.204-7	SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS	OCT 2018
52.204-13	SYSTEM FOR AWARD MANAGEMENT MAINTENANCE	OCT 2018
52.204-15	SERVICE CONTRACT REPORTING REQUIREMENTS FOR INDEFINITE-DELIVERY CONTRACTS	OCT 2016
52.204-22	ALTERNATIVE LINE ITEM PROPOSAL	JAN 2017
52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES	JUL 2018

52.207-6	SOLICITATION OF OFFERS FROM SMALL BUSINESS CONCERNS AND SMALL BUSINESS TEAMING ARRANGEMENTS OR JOINT VENTURES (MULTIPLE-AWARD CONTRACTS)	OCT 2016
52.209-6	PROTECTING THE GOVERNMENTS INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	OCT 2015
52.209-9	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	OCT 2018*
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.210-1	MARKET RESEARCH	APR 2011
52.215-2	AUDIT AND RECORDS – NEGOTIATION	OCT 2010
52.215-8	ORDER OF PRECEDENCE – UNIFORM CONTRACT FORMAT	OCT 1997
52.215-23	LIMITATIONS ON PASS-THROUGH CHARGES	OCT 2009
52.216-7	ALLOWABLE COST AND PAYMENT	AUG 2018
52.216-8	FIXED FEE	JUN 2011
52.217-2	CANCELLATION UNDER MULTI-YEAR CONTRACTS	OCT 1997
52.217-8	OPTION TO EXTEND SERVICES	NOV 1999
52.219-6	NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE	NOV 2011
52.219-14	LIMITATIONS ON SUBCONTRACTING	JAN 2017
52.222-2	PAYMENT FOR OVERTIME PREMIUMS	JUL 1990
52.222-21	PROHIBITION OF SEGREGATED FACILITIES	APR 2015
52.222-26	EQUAL OPPORTUNITY	SEP 2016
52.222-29	NOTIFICATION OF VISA DENIAL	APR 2015
52.222-50	COMBATING TRAFFICKING IN PERSONS	JAN 2019
52.223-6	DRUG-FREE WORKPLACE	MAY 2001
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	AUG 2011
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	JUN 2008
52.227-14	RIGHTS IN DATA-GENERAL	MAY 2014
52.228-3	WORKERS' COMPENSATION INSURANCE (DEFENSE BASE ACT)	JUL 2014
52.229-6	TAXES – FOREIGN FIXED-PRICE CONTRACTS	FEB 2013
52.229-8	TAXES – FOREIGN COST-REIMBURSEMENT CONTRACTS	MAR 1990
52.230-6	ADMINISTRATION OF COST ACCOUNTING STANDARDS	JUN 2010
52.232-1	PAYMENTS	APR 1984
52.232-8	DISCOUNTS FOR PROMPT PAYMENT	FEB 2002
52.232-11	EXTRAS	APR 1984
52.232-17	INTEREST	MAY 2014
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-20	LIMITATION OF COST	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.232-23	ASSIGNMENT OF CLAIMS	MAY 2014
52.232-25	PROMPT PAYMENT	JAN 2017
52.232-25	PROMPT PAYMENT – ALTERNATE I	FEB 2002
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER – SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	DEC 2013
52.233-1	DISPUTES	MAY 2014
52.233-3	PROTEST AFTER AWARD	AUG 1996

52.233-3	PROTEST AFTER AWARD – ALTERNATE I	JUN 1985
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.242-1	NOTICE OF INTENT TO DISALLOW COSTS	APR 1984
52.242-3	PENALTIES FOR UNALLOWABLE COSTS	MAY 2014
52.242-4	CERTIFICATION OF FINAL INDIRECT COSTS	JAN 1997
52.242-5	PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	JAN 2017
52.242-13	BANKRUPTCY	JUL 1995
52.242-17	GOVERNMENT DELAY OF WORK	APR 1984
52.243-1	CHANGES – FIXED-PRICE – ALTERNATE III	APR 1984
52.243-2	CHANGES – COST-REIMBURSEMENT – ALTERNATE I	APR 1984
52.244-2	SUBCONTRACTS	OCT 2010
52.244-2	SUBCONTRACTS – ALTERNATE I	JUNE 2007
52.244-5	COMPETITION IN SUBCONTRACTING	DEC 1996
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	AUG 2019
52.246-4	INSPECTION OF SERVICES – FIXED-PRICE	AUG 1996
52.246-5	INSPECTION OF SERVICES – COST-REIMBURSEMENT	APR 1984
52.246-25	LIMITATION OF LIABILITY – SERVICES	FEB 1997
52.247-63	PREFERENCE FOR U.S.-FLAG AIR CARRIERS	JUN 2003
52.249-1	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE) (SHORT FORM)	APR 1984
52.249-2	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE)	APR 2012
52.249-6	TERMINATION (COST-REIMBURSEMENT)	MAY 2004
52.249-8	DEFAULT (FIXED-PRICE SUPPLY AND SERVICE)	APR 1984
52.249-14	EXCUSABLE DELAYS	APR 1984
52.253-1	COMPUTER GENERATED FORMS	JAN 1991

* Will apply to the Contract if the Contractor checked “has” in paragraph (b) of the provision 52.209-7.

NUMBER	TITLE	DATE

AGENCY FOR INTERNATIONAL DEVELOPMENT ACQUISITION REGULATION (AIDAR)

752.202-1	DEFINITIONS	JAN 1990
752.209-71	ORGANIZATIONAL CONFLICTS OF INTEREST DISCOVERED AFTER AWARD	JUN 1993
752.211-70	LANGUAGE AND MEASUREMENT	JUN 1992
752.225-70	SOURCE AND NATIONALITY REQUIREMENTS	FEB 2012
752.227-14	RIGHTS IN DATA – GENERAL	OCT 2007
752.228-7	INSURANCE – LIABILITY TO THIRD PERSONS	JUL 1997
752.228-70	MEDICAL EVACUATION (MEDEVAC) SERVICES	JUL 2007
752.229-71	REPORTING OF FOREIGN TAXES	JUL 2007
752.231-71	SALARY SUPPLEMENTS FOR HG EMPLOYEES	MAR 2015
752.245-70	GOVERNMENT PROPERTY – USAID REPORTING REQUIREMENTS	OCT 2017
752.7001	BIOGRAPHICAL DATA	JUL 1997
752.7002	TRAVEL AND TRANSPORTATION	JAN 1990
752.7004	EMERGENCY LOCATOR INFORMATION	JUL 1997
752.7005	SUBMISSION REQUIREMENTS FOR DEVELOPMENT EXPERIENCE DOCUMENTS	SEP 2013
752.7006	NOTICES	APR 1984

752.7007	PERSONNEL COMPENSATION	JUL 2007
752.7008	USE OF GOVERNMENT FACILITIES OR PERSONNEL	APR 1984
752.7009	MARKING	JAN 1993
752.7010	CONVERSION OF U.S. DOLLARS TO LOCAL	APR 1984
752.7011	ORIENTATION AND LANGUAGE TRAINING	APR 1984
752.7013	CONTRACTOR-MISSION RELATIONSHIPS	JUN 2018
752.7014	NOTICE OF CHANGES IN TRAVEL REGULATIONS	JAN 1990
752.7015	USE OF POUCH FACILITIES	JUL 1997
752.7025	APPROVALS	APR 1984
752.7027	PERSONNEL	DEC 1990
752.7028	DIFFERENTIAL AND ALLOWANCES	JUL 1996
752.7029	POST PRIVILEGES	JUL 1993
752.7031	LEAVE AND HOLIDAYS	OCT 1989
752.7032	INTERNATIONAL TRAVEL APPROVAL AND NOTIFICATION REQUIREMENTS	APR 2014
752.7033	PHYSICAL FITNESS	JUL 1997
752.7034	ACKNOWLEDGMENT AND DISCLAIMER	DEC 1991
752.7036	USAID IMPLEMENTING PARTNER NOTICES (IPN) PORTAL FOR ACQUISITION	JUL 2014
752.7037	CHILD SAFEGUARDING STANDARDS	AUG 2016
752.7038	NONDISCRIMINATION AGAINST END-USERS OF SUPPLIES OR SERVICES	OCT 2016

I.2 AIDAR 752.245-70 – GOVERNMENT PROPERTY – USAID REPORTING REQUIREMENTS (OCTOBER 2017)

(a)

(1) The term Government-furnished property, wherever it appears in the following clause, shall mean (i) non-expendable personal property owned by or leased to the U.S. Government and furnished to the Contractor, and (ii) personal property furnished either prior to or during the performance of this Contract by any U.S. Government accountable officer to the Contractor for use in connection with performance of this Contract and identified by such officer as accountable. All mobile Information Technology (IT) equipment, including but not limited to, mobile phones (e.g. smartphones), laptops, tablets, and encrypted devices provided as government furnished property, title to which vests in the U.S. Government, are considered accountable personal property.

(2) The term Government property, wherever it appears in the following clause, shall mean Government-furnished property, Contractor acquired mobile IT equipment and non-expendable personal property title to which vests in the U.S. Government under this Contract.

(3) Non-expendable personal property, for purposes of this Contract, is defined as personal property that is complete in itself, does not lose its identity or become a component part of another article when put into use; is durable, with an expected service life of two years or more; and that has a unit cost of more than $500.

(b) Reporting Requirement: to be inserted following the text of the (48 CFR) FAR clause.

Reporting Requirements: The Contractor will submit an annual report on all nonexpendable property in a form and manner acceptable to USAID substantially as follows:

ANNUAL REPORT OF GOVERNMENT PROPERTY IN CONTRACTOR'S CUSTODY

		Furniture and Furnishings		
	Motor Vehicles	**Office**	**Living Quarters**	**Other Government**
A. Value of property as of last report				
B. Transactions during this reporting period				
(1) Acquisitions (add):				
a. Contractor acquired property[1]				
b. Government furnished[2]				
c. Transferred from others, without reimbursement[3]				
(2) Disposals (deduct):				
a. Returned to USAID				
b. Transferred to USAID—Contractor purchased				
c. Transferred to other Government agencies[3]				
d. Other disposals[3]				
C. Value of property as of reporting date				
D. Estimated average age of Contractor held property				
	Years	**Years**	**Years**	**Years**

[1] Non-expendable property and all mobile IT equipment.
[2] Government furnished property listed in this Contract as nonexpendable or accountable, including all mobile IT equipment.
[3] Explain if transactions were not processed through or otherwise authorized by USAID.

PROPERTY INVENTORY VERIFICATIONS

I attest that:

(1) Physical inventories of Government property are taken not less frequently than annually;
(2) The accountability records maintained for Government property in our possession are in agreement with such inventories; and
(3) The total of the detailed accountability records maintained agrees with the property value shown opposite line C above, and the estimated average age of each category of property is as cited opposite line D above.

_____
Authorized Signature

I.3 FAR 52.203-19 – PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

(a) *Definitions*. As used in this clause:

- "Internal confidentiality agreement or statement" means a confidentiality agreement or any other written statement that the Contractor requires any of its employees or subcontractors to sign regarding nondisclosure of Contractor information, except that it does not include confidentiality

agreements arising out of civil litigation or confidentiality agreements that Contractor employees or subcontractors sign at the behest of a Federal agency.

- "Subcontract" means any Contract as defined in subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a Prime Contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.
- "Subcontractor" means any supplier, distributor, vendor, or firm (including a consultant) that furnishes supplies or services to or for a Prime Contractor or another subcontractor.

(b) The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government Contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(c) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(d) The prohibition in paragraph (b) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(e) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235), and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such Contracts.

I.10 FAR 52.222-36 – EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)

(a) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of $15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

I.11 FAR 52.252-2 – CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This Contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: https://www.acquisition.gov/browse/index/far.

[END OF SECTION I]

Part II - Flow-down Clauses from USAID/*Collaboration, Learning, and Adapting (CLA)* Activity Contract # *72069622F00001*

SECTION D—PACKAGING AND MARKING

D.1 IDIQ Clauses Incorporated by Reference

This Task Order incorporates all clauses contained in Section D of basic IDIQ Contract No. 720-623-20-D-00005. See Excerpts from IDIQ Contract No. 72062320D00005.

D.2 Branding Implementation and Marking Plan

(a) Pursuant to **Section F.9.3**, the Contractor will submit a draft Branding Implementation Plan and Marking Plan as part of an overall communication strategy for TOCOR approval after Task Orderaward.

(b) The Contractor must comply with the requirements of the policy directives and required proceduresoutlined in USAID Automated Directive System ("ADS") 320.3.2 "Branding and Marking in USAID Direct Contracting" at http://www.usaid.gov/policy/ads/300/320.pdf; and USAID "GraphicStandards Manual" available at www.usaid.gov/branding, or any successor branding policy.

END OF SECTION D

SECTION E—INSPECTION AND ACCEPTANCE

E.1 Notice Listing Contract Clauses Incorporated by Reference

The following contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with FAR § 52.252-2, "Clauses Incorporated By Reference," in Section I of this contract.

NUMBER	TITLE	DATE
Federal Acquisition Regulation (48 CFR Chapter 1)		
52.246-3	Inspection of Supplies—Cost Reimbursement	MAY 2001

E.2 IDIQ Clauses Incorporated by Reference

This Task Order incorporates all clauses contained in Section E of basic IDIQ Contract No. 720-623-20-D-00005.

E.3 Inspection and Acceptance

(a) USAID inspection and acceptance of services, reports, and other required

deliverables or outputs will take place at the following location: **USAID/Rwanda, 30 KG 7 Avenue, Kacyiru, P.O. Box2848, Kigali, Rwanda.**

(b) USAID reserves the right to inspect and accept any services, reports, and other required deliverables or outputs where the services are performed and where reports and deliverables or outputs are produced or submitted. The TOCO has delegated authority to inspect and accept all services, reports,and required deliverables or outputs to the TOCOR, designated in **Section G** of this Task Order. TheTOCOR's acceptance of services, reports, and other deliverables may form the basis for payments tothe Contractor.

E.4 Performance Standards

USAID will evaluate the Contractor's performance in accordance with FAR § 42.15, corresponding USAID procedures, and the contractor's adherence to the annual work plan, reporting against its Monitoring & Evaluation Plan, and quality of reports described in Section F below. USAID will evaluate the contractor's performance during the initial, intermediate, and final periods of the contract in accordance with the Contractor Performance Assessment Reporting System ("CPARS"). The TOCO and the TOCOR will jointlyconduct the evaluation of the contractor's overall performance. This evaluation will form the basis of the contractor's permanent performance record under this contract.

END OF SECTION E

SECTION H – SPECIAL TASK ORDER REQUIREMENTS

H.1 IDIQ Clauses Incorporated by Reference

This Task Order incorporates all clauses contained in Section H of basic IDIQ Contract No. 720-623-20-D-00005. See Excerpts from IDIQ Contract No. 72062320D00005.

H.4 Authorized Geographic Code

(a) The Authorized Geographic Code for procurement of goods and services under this Task Order is
935.

(b) Authorized Geographic Code **935** includes any area or country, including the recipient country, butexcluding any country that is a prohibited source. USAID maintains a list of developing countries, advanced developing countries, and prohibited sources in ADS Chapter 310.

H.5 Language Requirements

(c) The Contractor will produce all reports and deliverables in standard English unless otherwiseauthorized in writing by the TOCOR.

(d) The Contractor must ensure that the Contractor's employees and consultants possess the appropriate level of skill in written and spoken English and local language proficiency, as needed, to perform theTask Order requirements.

H.6 Confidentiality and Ownership of Intellectual Property

Consistent with FAR § 52.227-14, Rights in Data – General, the Contractor must consider all reports generated during the performance of this Task Order as the property of USAID. During the term of this contract, the Contractor must not reproduce, disseminate, or discuss in open forum, other than for the purposes of completing the tasks described in Section C, these reports, or any findings based on data firstproduced in the performance of this contract, without the express written approval of the TOCOR.

H.8 AAPD 16-02 Revision 2 (R2) 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 anyequipment 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 inthis clause without the prior written approval by the Task Order 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'srequirements or to facilitate activities in the Government's statement of work, the Contractor must request prior written approval from the Task Order Contracting

Officer. (2) As part of the request, the Contractor must provide the Task Order 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 Task Order Contracting Officer's Representative (TOCOR) and the Office ofthe Chief Information Officer at ITAuthorization@usaid.gov. (e) The Task Order 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 TOCOR and the Agency CIO. The Task Order Contracting Officer will include the applicable clauses and special contract requirements in the modification. (f) Except as specified in the Task Order Contracting Officer's written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for informationtechnology as defined in this clause. (g) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

H.10 ADS 302.3.5.19 USAID-Financed Third-Party Web Sites (November 2017)

(a) Definitions:

"Third-party web sites" Sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of a contract. Third-partyWeb sites include project sites.

(b) The Contractor must adhere to the following requirements when developing, launching, and maintaininga third-party Web site funded by USAID for the purpose of meeting the project implementation goals:

(1) Prior to Web site development, the Contractor must provide information as required in Section C-Statement of Work of the contract (including a copy of the Contractor's privacy policy) to the Task Order Contracting Officer's Representative (TOCOR) for USAID's Bureau for Legislative andPublic Affairs (LPA) evaluation and approval. The Contractor must notify the COR of the Web site URL as far in advance of the site's launch as possible and must not launch the Web site until USAID's (LPA) approval has been provided through the COR. The Contractor must provide the COR with any changes to the privacy policy for the duration of the contract.

(2) The Contractor must collect only the amount of information necessary to complete the specificbusiness need as required by statute, regulation, or Executive Order.

(3) The Contractor must comply with Agency branding and marking requirements comprised of theUSAID logo and brandmark with the tagline "from the American people," located on the USAID Web site at www.usaid.gov/branding, and USAID Graphics Standards manual at http://www.usaid.gov.

(4) The Web site must be marked on the index page of the site and every major entry point to the Website with a disclaimer that states: "The information provided on this Web site is not official U.S. Government information and does not represent the views or positions of the U.S. Agency for International Development or the U.S. Government."

(5) The Web site must provide persons with disabilities access to information that is comparable to the access available to others. As such, all site content must be compliant with the requirements of theSection 508 amendments to the Rehabilitation Act.

(6) The Contractor must identify and provide to the COR, in writing, the contact information for the information security point of contact. The Contractor is responsible for updating the contact information whenever there is a change in personnel assigned to this role. Text highlighted in yellowindicates that the material is new or substantively revised.

(7) The Contractor must provide adequate protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted on the Web sites. To minimize security risks and ensure the integrity and availability of information, the Contractor must use sound:system/software management; engineering and development; and secure coding practices consistent with USAID standards and information security best practices. Rigorous security safeguards, including but not limited to, virus protection; network intrusion detection and prevention programs; and vulnerability management systems must be implemented, and critical security issues must be resolved as quickly as possible or within 30 days. Contact the USAID Chief Information Security Officer (CISO) at ISSO@usaid.gov for specific standards and guidance.

(8) The Contractor must conduct periodic vulnerability scans, mitigate all security risks identified during such scans, and report subsequent remediation actions to CISO at ISSO@usaid.gov and CORwithin 30 workdays from the date vulnerabilities are identified. The report must include disclosure of the tools used to conduct the scans. Alternatively, the contractor may authorize USAID CISO at ISSO@usaid.gov to conduct periodic vulnerability scans via its Web-scanning program. The sole purpose of USAID scanning will be to minimize security risks. The Contractor will be responsible for taking the necessary remediation action and reporting to USAID as specified above.

(c) For general information, agency graphics, metadata, privacy policy, and Section 508 compliancerequirements, refer to http://www.usaid.gov.

H.11 Environmental Compliance

1) The Foreign Assistance Act of 1961, as amended, Section 117 requires that the impact of USAID's activities on the environment be considered and that USAID include environmental sustainability as a centralconsideration in designing and carrying out its development programs. This mandate is codified in Federal Regulations (22 CFR 216) and in USAID's Automated Directives System (ADS) ADS 201 and ADS 204, which, in part, require that the potential environmental impacts of USAID-financed activities are identified prior to a final decision to proceed and that appropriate environmental safeguards are adopted for all activities. Contractor's environmental compliance obligations under these regulations and procedures are specified in the following paragraphs of this Task Order.

2) In addition, the Contractor must comply with host country environmental regulations unless otherwisedirected in writing by USAID. In case of conflict between host country

and USAID regulations, the lattershall govern.

3) No activity funded under this Task Order must be implemented unless an environmental threshold determination, as defined by 22 CFR 216, has been reached for that activity, as documented in a Request forCategorical Exclusion (RCE), Initial Environmental Examination (IEE), or Environmental Assessment (EA)duly signed by the Bureau Environmental Officer (BEO). (Hereinafter, such documents are described as "approved Regulation 216 environmental documentation.")

4) As part of its Initial and all Annual Work Plans thereafter, the Contractor, in collaboration with the USAID TOCOR and Mission Environmental Officer or Bureau Environmental Officer, as appropriate, shallreview all ongoing and planned activities under this award to determine if they are within the scope of the approved Regulation 216 environmental documentation.

5) If the Contractor plans any new activities outside the scope of the approved Regulation 216 environmentaldocumentation, it shall prepare an amendment to the documentation for USAID review and approval. No such new activities shall be undertaken prior to receiving written USAID approval of environmental documentation amendments.

6) Any ongoing activities found to be outside the scope of the approved Regulation 216 environmental documentation shall be halted until an amendment to the documentation is submitted and written approval isreceived from USAID.

H.13 Organizational Conflicts of Interest Discovered After Award

(e) The Contractor agrees that, if after award it discovers either an actual, apparent, or potential organizational conflict of interest ("OCI") with respect to this contract, it must make an immediate and full disclosure in writing to the TOCO which must include a description of the action(s) whichthe Contractor has taken or proposes to take to avoid, eliminate or neutralize the conflict.

(f) The TOCO will provide the contractor with written instructions concerning the conflict. USAID reserves the right to terminate the contract if such action is determined to be in the best interests ofthe Government.

H.14 Organizational Conflicts of Interest: Preclusion from Furnishing Certain Services andRestrictions on Use of Information

(g) This Task Order requires the Contractor to furnish important services in support of the monitoring and evaluation of USAID/Rwanda's portfolio. In accordance with FAR Subpart 9.5, the Contractor remains ineligible to furnish, as a prime or subcontractor, implementation services under any USAIDaward that results in response to findings, proposals, or recommendations in the evaluation report within 18 months of USAID accepting the report, unless USAID waives such requirements (in accordance FAR § 9.503 determining that preclusion of the Contractor from the implementation work would not serve USAID's interest).

(h) In addition, through the execution of this Task Order, the Contractor agrees that it

will not use ormake available any information obtained about another organization under the Task Order in thepreparation of proposals or other documents in response to any solicitation.

(i) If the contractor gains access to proprietary information of other organizations in performing its monitoring and evaluation services, the Contractor must agree with the other organizations to protecttheir information from unauthorized use or disclosure for as long as it remains proprietary and must refrain from using the information for any purpose other than that for which it was furnished. The Contractor must provide a properly executed copy of all such agreements to the COR.

END OF SECTION H

PART II – CONTRACT CLAUSES

SECTION I – TASK ORDER

CLAUSES

I.1 APPLICABILITY OF IDIQ CONTRACT CLAUSES

As applicable, all Clauses from the basic IDIQ apply to this Task Order and shall be in full force and effect.The following clauses of the aforesaid IDIQ are inserted herein in their most updated format:

FEDERAL ACQUISITION

FEDERAL ACQUISITION REGULATION
(48 CFR Chapter 1)

NUMBER	TITLE	DATE
52.202-1	DEFINITIONS	(JUN 2020)
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	(JUN 2020)
52.203-7	ANTI-KICKBACK PROCEDURES	(JUN 2020)
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	(JUN 2020)
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	(JUN 2020)
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS	(JUN 2020)
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	(JUN 2020)
52.210-1	MARKET RESEARCH	(JUN 2020)
52.215-2	AUDIT AND RECORDS—NEGOTIATION	(JUN 2020)
52.215-11	PRICE REDUCTION FOR DEFECTIVE CERTIFIED COST OR PRICING DATA—MODIFICATIONS	(JUN 2020)
52.215-13	SUBCONTRACTOR CERTIFIED COST OR PRICING	

	DATA—MODIFICATIONS	(JUN 2020)
52.215-14	INTEGRITY OF UNIT PRICES	(JUN 2020)
52.215-23	LIMITATIONS ON PASS-THROUGH CHARGES	(JUN 2020)
52.219-7	NOTICE OF PARTIAL SMALL BUSINESS SET-ASIDE	(NOV 2020)
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	(JUN 2020)
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES	(JUN 2020)
52.222-37	EMPLOYMENT REPORTS ON VETERANS	(JUN 2020)
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	(JUN 2020)
52.230-2	COST ACCOUNTING STANDARDS	(JUN 2020)
52.230-3	DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES	(JUN 2020)
52.230-4	DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES PRACTICES-FOREIGN CONCERNS	(JUN 2020)
52.244-2	SUBCONTRACTS	(JUN 2020)
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	(NOV 2020)

I.2 FAR 52.203-13 CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (JUNE 2020)

(a) *Definitions. As used in this clause—*

Agent means any individual, including a director, an officer, an employee, or an independent Contractor,authorized to act on behalf of the organization.

Full cooperation-

i. Means disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response toGovernment auditors' and investigators' request for documents and access to employees with information;

ii. Does not foreclose any Contractor rights arising in law, the FAR, or the terms of thecontract. It does not require-

(i) A Contractor to waive its attorney-client privilege or the protections afforded by the attorneywork product doctrine; or
(ii) Any officer, director, owner, or employee of the Contractor, including a sole proprietor, to waivehis or her attorney client privilege or Fifth Amendment rights; and

iii. Does not restrict a Contractor from-

(i) Conducting an internal investigation; or
(ii) Defending a proceeding or dispute arising under the contract or related to a potential or disclosedviolation.

Principal means an officer, director, owner, partner, or a person having primary management or supervisoryresponsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or businesssegment; and similar positions).

Subcontract means any contract entered into by a subcontractor to furnish supplies or services forperformance of a prime contract or a subcontract.

Subcontractor means any supplier, distributor, vendor, or firm that furnished supplies or services to or for aprime contractor or another subcontractor.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) *Code of business ethics and conduct.*

(1) Within 30 days after contract award, unless the Contracting Officer establishes a longer time period,the Contractor shall-

(i) Have a written code of business ethics and conduct; and
(ii) Make a copy of the code available to each employee engaged in performance of the contract.

(2) *The Contractor shall-*

(i) Exercise due diligence to prevent and detect criminal conduct; and
(ii) Otherwise promote an organizational culture that encourages ethical conduct and a commitmentto compliance with the law.

(3)

(i) The Contractor shall timely disclose, in writing, to the agency Office of the Inspector General(OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed-

(A) A violation of Federal criminal law involving fraud, conflict of interest, bribery, orgratuity violations found in Title 18 of the United States Code; or
(B) A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(ii) The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the company. To the extent permitted by law and regulation, such information will not be released by the Government to thepublic pursuant to a Freedom of Information Act request, 5 U.S.C. Section 552, without prior notification to the Contractor. The Government may transfer documents provided by the Contractor to any department or agency within the Executive Branch if the information relates tomatters within the organization's jurisdiction.

(iii) If the violation relates to an order against a Government-wide acquisition contract, a multi- agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or anyother procurement instrument intended for use by multiple agencies, the Contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract.

(c) Business ethics awareness and compliance program and internal control system. This paragraph (c) doesnot apply if the Contractor has represented itself as a small business concern pursuant to the award of this contract or if this contract is for the acquisition of a commercial item as defined at FAR 2.101. The Contractor shall establish the following within 90 days after contract award, unless the Contracting Officer establishes a longer time period:

(1) An ongoing business ethics awareness and compliance program.

(i) This program shall include reasonable steps to communicate periodically and in a practical manner the Contractor's standards and procedures and other aspects of the Contractor's businessethics awareness and compliance program and internal control system, by conducting effective training programs and otherwise disseminating information appropriate to an individual's respective roles and responsibilities.

(ii) The training conducted under this program shall be provided to the Contractor's principalsand employees, and as appropriate, the Contractor's agents and subcontractors.

(2) An internal control system.

(i) The Contractor's internal control system shall—

(A) Establish standards and procedures to facilitate timely discovery of improperconduct in connection with Government contracts; and

(B) Ensure corrective measures are promptly instituted and carried out.

(ii) At a minimum, the Contractor's internal control system shall provide for the following:

(A) Assignment of responsibility at a sufficiently high level and adequate resources toensure effectiveness of the business ethics awareness and compliance program and internal control system.

(B) Reasonable efforts not to include an individual as a principal, whom due diligencewould have exposed as having engaged in conduct that is in conflict with the Contractor's code of business ethics and conduct.

(C) Periodic reviews of company business practices, procedures, policies, and internalcontrols for compliance with the Contractor's code of business ethics and conduct andthe special requirements of Government contracting, including-

(1) Monitoring and auditing to detect criminal conduct;
(2) Periodic evaluation of the effectiveness of the business ethics awareness and compliance program and internal control system, especially if criminal conduct hasbeen detected; and
(3) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business ethics awareness and compliance program and the internal control system as necessary to reduce the risk of criminal conduct identified through this process.

(D) An internal reporting mechanism, such as a hotline, which allows for anonymity or confidentiality, by which employees may report suspected instances of improper conduct,and instructions that encourage employees to make such reports.

(E) Disciplinary action for improper conduct or for failing to take reasonable steps toprevent or detect improper conduct.

(F) Timely disclosure, in writing, to the agency OIG, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violationof the civil False Claims Act (31 U.S.C. 3729-3733).

(1) If a violation relates to more than one Government contract, the Contractor maymake the disclosure to the agency OIG and Contracting Officer responsible for the largest dollar value contract impacted by the violation.
(2) If the violation relates to an order against a Governmentwide

acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the contractor shall notify the OIG of the ordering agency and theIG of the agency responsible for the basic contract, and the respective agencies' contracting officers.
(3) The disclosure requirement for an individual contract continues until at least 3years after final payment on the contract.
(4) The Government will safeguard such disclosures in accordance with paragraph(b)(3)(ii) of this clause.

(G) Full cooperation with any Government agencies responsible for audits, investigations, orcorrective actions.

(d) *Subcontracts*.

(1) The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts that exceed the threshold specified in FAR 3.1004(a) on the date of subcontract award and aperformance period of more than 120 days.

(2) In altering this clause to identify the appropriate parties, all disclosures of violation of the civil FalseClaims Act or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the Contracting Officer.

I.4 FAR 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FORFEDERAL CONTRACTORS (OCT 2021) (DEVIATION #M/OAA-DEV-FAR-22-01c)

(a) Definition. As used in this clause - United States or its outlying areas means—

(1) The fifty States;
(2) The District of Columbia;
(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;
(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and
(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID SafetyProtocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor or subcontractor workplaces published by the Safer Federal Workforce Task Force (Task Force Guidance) at https://www.saferfederalworkforce.gov/contractors/. While at a USAID workplace, covered contractor employees must also comply with any additional agency workplace safety requirements for that workplace that are applicable to federal employees, asamended (see USAID's COVID-19 Safety Plan and

Workplace Guidelines (Safety Plan).

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part in the United States or its outlying areas.

END OF SECTION I

SAM.GOV®

Quick Start Guide for International Registrations

How to Start Registering an International Entity in SAM.gov

SAM.gov is an official website of the United States government. There is NO charge to register or maintain your entity registration record in SAM.gov.

What is an entity?

The term "entity" refers to prime contractors, organizations or individuals applying for assistance awards, those receiving loans, sole proprietors, corporations, partnerships, and any U.S. federal government agencies desiring to do business with the government. "Entity" can also refer to a party that has been suspended or debarred, is covered by a prohibition or restriction, or is otherwise excluded from doing business with the government.

An international entity refers to an entity that is based outside of the United States.

What is entity registration?

An entity registration allows you to bid on U.S. government contracts and apply for federal assistance. We will assign you a Unique Entity ID (SAM) as part of entity registration.

Comprehensive and current entity information is essential for the federal award process. It is important to prepare your information and allow sufficient time to understand and accurately complete your registration. You only need to complete and manage it here to remain eligible for federal awards. You must renew your registration every 365 days for it to remain active.

What do I need to get started?

Before starting a registration, international entities must obtain an NCAGE Code for each entity they plan to register in SAM.gov. Get an NCAGE Code here. Make sure the legal business name and physical address you provide to get your NCAGE Code and register are identical. It takes up to 3 business days to obtain a NCAGE code.

Registrations require you to enter a lot of information about your entity. Information includes, but is not limited to your:

- entity's legal business name
- physical address
- tax identification number (TIN)–*only needed if your entity pays U.S. taxes*
- NCAGE code
- information about the types of goods and services you provide
- entity size
- optional Electronic Data Interchange (EDI) information

- disaster relief data
- representations and certifications
- points of contact

Visit the **Get Started** page at SAM.gov to view checklists and guides to help you prepare for registration. If you already have a Unique Entity ID but have not completed registration, go to this section.

Start Registration

When you are ready to start a new entity registration, go to SAM.gov and follow these steps:

1. Select the "Sign In" link at the upper right corner of the page. Select "Accept" to accept the U.S. Government System terms. After selecting "Accept," the system will redirect you to login.gov.
2. Login.gov is a service that manages usernames and passwords for SAM.gov. If you already have a login.gov account, sign in with your credentials. Otherwise, select "Create An Account" and follow the prompts.
3. Once you are signed in, the system will redirect you to your SAM.gov Workspace.
4. On the "Entity Management" widget in the Workspace, select the "Get Started" button.
5. On the next page, select the "Register Entity" button.
6. On the next page, you will choose your entity type and your "Purpose of Registration."
    a. Select your type of entity. Choose "Business or Organization" if you are NOT a U.S. State, U.S. Local, Tribal, or Foreign government entity.
    b. There are two types of registration purposes: Financial Assistance Awards and All Awards.
        i. An All Awards registration allows you to bid on contracts and other procurements, as well as apply for financial assistance. This type of registration requires more information.
        ii. A Financial Assistance Awards registration allows you to apply for financial assistance, or grants and loans, **only**. This type of registration requires less information.
    c. Select your registration purpose, then select "Next."
7. The next two pages display your choices from the Purpose of Registration page and a summary of the information you need to have prepared to complete your registration. Review the pages to make sure you are ready to start. Confirm your selections and select "Go back" if you need to change your purpose of registration or entity type. If your information is correct, select "Next."
8. Here you will start to enter information about your entity. Enter your legal business name and physical address, then select "Next."
9. Your entity name and address will be validated by SAM.gov. The next page will show an entity matched in SAM.gov. If your entity information is correct, select "Next."
    a. If the match shown is not your entity or you are unable to find a match, you can create a help ticket with the Federal Service Desk (FSD) from the page. Select the "Create Incident" button to contact the FSD for assistance.

10. On this page, you will choose whether to allow your entity record to be publicly displayed in SAM.gov. Note that if you deselect this box and restrict the public display of your entity, only you and federal government users will be able to view your entity record.
11. Then, you must certify under penalty of law that you are authorized to conduct transactions for the entity. Then, select "Receive Unique Entity ID."
12. The next page will display your Unique Entity ID. If the entity already has a registration or a Unique Entity ID, you will see informational alerts at the top of the page with more details.
13. Select "Continue Registration" to go to the next registration step. If you select "Done," you will be redirected to your Workspace. You can continue registration later if you choose to.

Continuing Registration

When you select "Continue Registration" from the "Receive Unique Entity ID" page, the remaining sections of registration will be displayed. Select "Continue" to begin entering information into the Core Data section of registration. Visit the **Get Started** page at SAM.gov to view checklists and guides to help you prepare for registration.

1. Enter additional organization information as required. You will create a Marketing Partner Identification Number (MPIN) on this page. It is **important to remember your MPIN** as it will serve as your electronic signature for the IRS Consent to Disclosure of Tax Information on the next page. You will need your MPIN in the future to make updates to your registration.

Continue to enter additional information into each section as required. Your information will be saved when you select "Save and Continue" on each page.

If you exit registration before completing it, you can access it later from your Workspace.

1. Sign in to SAM.gov and, in the Workspace, select the "Work in Progress" bubble on the "Entity Management" widget. A list of your registrations in progress will display.
2. Next to the record title you want to access, select the button with the three dots (the Actions menu), then choose "Update" from the menu. You will be redirected to where you left off in your registration.
    a. If you do not access or submit your registration within 90 days, the system will remove it.

After entering and reviewing your information, select the "Submit" button. You will receive a "Registration Submitted – Confirmation" message on the screen. If you do not see this message, you have not submitted your registration.

When will my registration become active?

Allow at least **ten business days** after you submit your registration for it to become active in SAM.gov. If your entity fails TIN or NCAGE code validation, SAM.gov will send you an email with instructions on updating your information and resubmitting your registration. You may need to work with the IRS or NCAGE to update your information before resubmitting your registration.

How do I check the status of my entity registration?

If you have a role with an entity and are signed in to your SAM.gov account, you can check your entity registration status. You can also check the status of an entity's registration as a federal user. If none of these is the case, you cannot check an entity's registration status.

1. Sign in to SAM.gov. You must be signed in to check your registration status.
2. From the home page, select the "Check Registration Status" button. The page is also linked in the footer of all pages on SAM.gov.
3. Enter a Unique Entity ID or NCAGE Code and select "Search." The entity's registration status will display below.