Annex E

SPECIAL CONTRACTING REQUIREMENTS

The Contractor will be bound by the terms and conditions of its GSA MAS contract No. 47QRAA23D003U in addition to any terms in this section.

1. NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

752.252-1 AIDAR SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (MAR 2015)

This solicitation incorporates one or more provisions 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 all AIDAR solicitation provisions is contained in the Code of Federal Regulations (CFR) located at 48 CFR Chapter 7. The following AIDAR clause pertinent to this section is hereby incorporated by reference (by Citation Number, Title, and Date).

NUMBER	TITLE	DATE
752.7004	Emergency Locator Information	JUL 1997
752.7027	Personnel	DEC 1990

2. AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this contract is 937. Please see ADS 310 for further details.

3. CONFIDENTIALITY AND OWNERSHIP OF INTELLECTUAL PROPERTY

All reports generated and data collected during this project must be considered the property of USAID and must not be reproduced, disseminated, or discussed in open forum, other than for the purposes of completing the tasks described in this document, without the express written approval of a duly-authorized representative of USAID. All findings, conclusions and recommendations must be considered confidential and proprietary.

4. DISCLOSURE OF INFORMATION

(a) 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.

(b) 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 must be under the supervision of the Contractor or the Contractor's responsible employees.

(c) 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 extend 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, must be guilty of a crime punishable by a fine of up to $10,000, or imprisoned up to ten years, or both.

5. ETHICS

The Contractor/Vendor must ensure that the Contractors provided to USAID must be legally bound and must be made aware that the following USAID rules regarding ethical conduct must apply to such Contractors. The Contractors provided to USAID are not employees of the U.S. Government. However, in order to avoid both an actual conflict and/or the appearance of a conflict of interest between such Contractors' duties on behalf of the U.S. Government and any outside activity pursued by such Contractors or any activity of the organizations employing the Contractors, such Contractors will be subject to the standards of ethical conduct for Government employees, except that such Contractors will be subject to the standards of ethical conduct for Government employees, except that such Contractors will not be required, except that such Contractors will not be required to file a financial disclosure statement.

6. EXECUTIVE ORDER ON TERRORISM FINANCING

The Contractor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Contractor to ensure compliance with these Executive Orders and laws. This provision must be included in all subcontracts issued under this contract.

7. HANDLING OF DATA

(a) In the performance of this contract, it is anticipated that the Contractor may have access to, be furnished with or use the following categories of data (which may be technical data, administrative, management information, or financial, including cost or pricing):

i. Data of third parties which the Government has agreed to handle under protective arrangements; and

ii. Government data, the use and dissemination of which, the Government intends to control.

(b) In order to protect the interests of the Government and the owners, licensors and licensees of such data, the Contractor agrees, with respect to any such third party or Government data that is either marked with a restrictive legends, specifically identified in this contract, or otherwise identified in writing by the Contracting Officer as being subject to this clause, to:

i. Use, disclose, and reproduce such data only to the extent necessary to perform the work required under this contract;

ii. Allow access to such data only to those of its employees that require access for their performance under this contract;

iii. Preclude access and disclosure of such data outside the Contractor’s organization; and

iv. Return or dispose of such data, as the Contracting Officer may direct, when the data is no longer needed for contract performance.

(c) The Contractor agrees to inform and instruct its employees of its and their obligations under this clause and to appropriately bind its employees contractually to comply with the access, use, disclosure, and reproduction provisions of this clause.

(d) In the event that data includes a legend that the Contractor deems to be ambiguous or unauthorized, the Contractor may inform the Contracting Officer of such condition. Notwithstanding such a legend, as long as such legend provides an indication that a restriction on use or disclosure was intended; the

Contractor must treat such data pursuant to the requirements of this clause unless otherwise directed, in writing, by the Contracting Officer.

(e) Notwithstanding the above, the Contractor must not be restricted in use, disclosure, and reproduction of any data that:
   i. Is or becomes, generally available or public knowledge without breach of this clause by the Contractor;
   ii. Is known to, in the possession of, or is developed by the Contractor independently of any disclosure of, or without reference to, proprietary, restricted, confidential, or otherwise protectable data under this clause;
   iii. Is rightfully received by the Contractor from a third party without restriction;
   iv. Or is required to be produced by the Contractor pursuant to a court order or other Government action.

If the Contractor believes that any of these events or conditions that remove restrictions on the use, disclosure, and reproduction of the data apply, the Contractor must promptly notify the Contracting Officer of such belief prior to acting on such belief, and, in any event, must give notice to the Contracting Officer prior to any unrestricted use, disclosure, or reproduction of such data.

8. Worker's Compensation Insurance (Defense Base Act) (DEC 1991) [(DEVIATION JUNE 2022)]

In addition to the requirements specified in (48 CFR) FAR 52.228-3, the contractor agrees to the following:
(a) The Contractor agrees to procure Defense Base Act (DBA) insurance pursuant to the terms of the contract between USAID and USAID's DBA insurance carrier unless the Contractor has a DBA self insurance program approved by the Department of Labor or has an approved retrospective rating agreement for DBA. The rates and contact information for USAID's DBA insurance carrier are published in an Acquisition & Assistance Policy Directive found on USAID's website: https://www.usaid.gov/partner-with-us/aapds-cibs. Alternatively, the Contractor can request the rates and contact information from the Contracting Officer.
(b) If USAID or the contractor has secured a waiver of DBA coverage (see (48 CFR) AIDAR 728.305-70(a)) for contractor's employees who are not citizens of, residents of, or hired in the United States, the contractor agrees to provide such employees with worker's compensation benefits as required by the laws of the country in which the employees are working, or by the laws of the employee's native country, whichever offers greater benefits.
(c) The Contractor further agrees to insert in all subcontracts hereunder to which the DBA is applicable, a clause similar to this clause, including this sentence, imposing on all subcontractors a like requirement to provide overseas worker's compensation insurance coverage and obtain DBA coverage under the USAID requirements contract.

9. INTERNATIONAL TRAVEL APPROVAL AND NOTIFICATION REQUIREMENTS (APR 2014) AIDAR 752.7032

Prior written approval by the Contracting Officer, or the Contracting Officer's Representative (COR) if delegated in the Contracting Officer's Representative Designation Letter, is required for all international travel directly and identifiably funded by USAID under this contract. The Contractor must therefore present to the contracting officer or the contracting officer's representative, an itinerary for each planned international trip, showing the name of the traveler, purpose of the trip, origin/destination (and intervening stops), and dates of travel, as far in advance of the proposed travel as possible, but in no event less than three weeks before travel is planned to commence. The contracting officer's or contracting officer's representative (if delegated by the contracting officer) prior written approval may be in the form of a letter or telegram or similar device or may be specifically incorporated into the schedule of the contract. At least one week prior to commencement of approved international travel, the Contractor must notify the cognizant Mission, with a copy to the contracting officer or contracting officer's representative, of planned travel, identifying the travelers and the dates and times of arrival.

10. MEDICAL EVACUATION (MEDEVAC) SERVICES (July 2007)

As prescribed in AIDAR 728.307-70, for use in all contracts requiring performance overseas:

(a) Contractors must provide MEDEVAC service coverage to all U.S. citizen, U.S. resident alien, and Third Country National employees and their authorized dependents (hereinafter "individual") while overseas under a USAID-financed direct contract. USAID will reimburse reasonable, allowable, and allocable costs for MEDEVAC service coverage incurred under the contract. The Contracting Officer will determine the reasonableness, allowability, and allocability of the costs based on the applicable cost principles and in accordance with cost accounting standards.

(b) Exceptions.
  (i) The Contractor is not required to provide MEDEVAC insurance to eligible employees and their dependents with a health program that includes sufficient MEDEVAC coverage as approved by the Contracting Officer.
  (ii) The Mission Director may make a written determination to waive the requirement for such coverage. The determination must be based on findings that the quality of local medical services or other circumstances obviate the need for such coverage for eligible employees and their dependents located at post.

(c) Contractor must insert a clause similar to this clause in all subcontracts that require performance by Contractor employees overseas.

11. NONDISCRIMINATION

Most federal Contractors are prohibited by law and regulation from discrimination with regard to race, color, religion, sex, national origin, disability, age, genetic information, or veteran status when work under their contract is performed in the U.S. or employees are recruited from the U.S. The requirements applicable to federal contracts are found in FAR Part 22, "Application of Labor Laws to Government Acquisitions" and the clauses in FAR Part 52.227.

Additionally, while not a mandatory requirement, the Agency encourages all organizations performing under USAID contracts, including those performed solely overseas, to apply these same standards of nondiscrimination to other bases, including sexual orientation, gender identity, pregnancy, and any other conduct that does not adversely affect performance, subject to applicable law.

12. ORGANIZATIONAL CONFLICTS OF INTEREST: PRECLUSION FROM FURNISHING CERTAIN SERVICES AND RESTRICTION ON USE OF INFORMATION (EVALUATION)

(1) This Contract may call for the Contractor to furnish services in support of evaluation of Contractors or of specific LAC Education activities. In accordance with the principles of FAR Subpart 9.5 and USAID policy, THE CONTRACTOR MUST 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, in consultation with USAID's Competition Advocate, 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.

(2) 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.

(3) 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 as furnished. THE CONTRACTOR MUST PROVIDE A PROPERLY EXECUTED COPY OF ALL SUCH AGREEMENTS TO THE CONTRACTING OFFICER.

13. ORGANIZATIONAL CONFLICTS OF INTEREST: PRECLUSION FROM IMPLEMENTATION CONTRACT (DESIGN SERVICES)

This contract may call for the Contractor to furnish important services in support of the design of specific LAC Education activities. In accordance with the principles of FAR Subpart 9.5 and USAID policy, THE CONTRACTOR SHALL BE INELIGIBLE TO FURNISH, AS A PRIME OR SUBCONTRACTOR OR OTHERWISE, THE IMPLEMENTATION SERVICES FOR ANY ACTIVITIES FOR WHICH IT PROVIDES SUBSTANTIAL DESIGN SERVICES EXCEPT FOR SUCH SERVICES THAT MAY BE FURNISHED UNDER THIS CONTRACT, unless the Head of the Contracting Activity, in consultation with USAID's Competition Advocate, authorizes a waiver (in accordance FAR 9.503) determining that preclusion of the Contractor from the implementation contract would not be in the Government's interest. When a task order includes a work requirement that will preclude the Contractor from furnishing implementation services, a clause stating the preclusion will be included in the task order.

14. PROHIBITION OF ASSISTANCE TO DRUG TRAFFICKERS

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

15. REPORTING OF FOREIGN TAXES (July 2007)

(a) Reports. The Contractor must annually submit an annual report by April 16 of the next year.

(b) Contents of Report. The reports must contain:
(1) Contractor name.
(2) Contact name with phone, fax and email.
(3) Agreement number(s).
(4) Amount of foreign taxes assessed by a foreign Government [*list each foreign government separately*] on commodity purchase transactions valued at $500 or more financed with U.S. foreign assistance funds under this agreement during the prior U.S. fiscal year.
(5) Only foreign taxes assessed by the foreign government in the country receiving U.S. assistance is to be reported. Foreign taxes by a third-party foreign government are not to be reported.
(6) Any reimbursements received by the Contractor during the period in (iv) regardless of when the foreign tax was assessed plus, for the interim report, any reimbursements on the taxes reported in (iv) received by the Contractor through October 31 and for the final report, any reimbursements on the taxes reported in (iv) received through March 31.
(7) The final report is an updated cumulative report of the interim report.
(8) Reports are required even if the Contractor/recipient did not pay any taxes during the report period.

(9) Cumulative reports may be provided if the Contractor/recipient is implementing more than one program in a foreign country.

(c) Definitions. For purposes of this clause:
(1) "Agreement" includes USAID direct and country Contracts, grants, cooperative agreements and interagency agreements.
(2) "Commodity" means any material, article, supply, goods, or equipment.
(3) "Foreign government" includes any foreign governmental entity.
(4) "Foreign taxes" means value-added taxes and custom duties assessed by a foreign government on a commodity. It does not include foreign sales taxes.

(d) Where. Submit the reports to: *vatreportswash@usaid.gov*

(e) Sub Agreements. The Contractor must include this reporting requirement in all applicable subcontracts, sub and other sub agreements.

(f) For further information see *http://2001-2009.state.gov/s/d/rm/c10443.htm*.

16. REPORTING WASTE, FRAUD, ABUSE AND THEFT

The Contractor shall notify the Contracting Officer and the COR of any instances of suspected waste, fraud, abuse, loss, or theft of Contractor or Government-furnished property by employees or Subcontractors.

17. USAID DISABILITY POLICY - ACQUISITION (DECEMBER 2004) (AAPD 04-17)

"USAID Disability Policy - Acquisition (December 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: *http://pdf.dec.org/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 make 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."

18. USAID IMPLEMENTATION OF SECTION 508 OF THE REHABILITATION ACT OF 1973 AND FEDERAL ACQUISITION CIRCULAR (FAC) 97-27 "ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

In accordance with ADS 302, Contractor shall comply with USAID Implementation of Section 508 of the Rehabilitation Act of 1973 and Federal Acquisition Circular (FAC) 97-27 "Electric and Information Technology Accessibility. Further information on Section 508 is available via the Internet at:

- *http://www.section508.gov*
- *http://www.usaid.gov/policy/ads/300/302.pdf*

19. 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.

20. LIMITATION ON ACQUISITION OF INFORMATION TECHNOLOGY (APRIL 2018) (DEVIATION NOs. M/OAA-DEV-FAR-20-3c and M/OAA-DEV-AIDAR-20-2c) (APRIL 2020)

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

1. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where
2. such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.
3. The term " information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.
4. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

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

technology or information technology services.
(c) The Contractor must not acquire information technology as defined in this clause without the prior written approval by the contracting officer as specified in this clause.
(d) Request for Approval Requirements:

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

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

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

(f) Except as specified in the contracting officer's written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for information technology as defined in this clause.
(g) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

21. MEDIA AND INFORMATION HANDLING AND PROTECTION (MAY 2016)

(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 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 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).

22. PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEMS INCIDENT REPORTING (MAY 2016)

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

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

"Sensitive Information" or "Sensitive But Unclassified" Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information

(TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS- 46;05-26-1995). SBU information includes, but is not limited to:

1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers, "Personally Identifiable Information (PII)", means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term "individual" refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

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

"Information Security and Privacy Incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

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

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

(d) IT Security and Privacy Training
(1) All Contractor personnel must complete USAID-provided mandatory security and privacy training prior to gaining access to USAID information systems and annually thereafter.
(2) The USAID Rules of Behavior must be signed by each user prior to gaining access to USAID information systems, periodically at the request of USAID, or whenever the Rules are updated. USAID will

provide access to the rules of behavior and provide notification as required.
(3) Security and privacy refresher training must be completed on an annual basis by all Contractor and subcontractor personnel providing support under this contract. USAID will provide notification and instructions on completing this training.
(4) Contractor employees filling roles identified by USAID as having significant security responsibilities must complete role-based training upon assignment of duties and thereafter at a minimum of every three years.
(5) Within fifteen (15) calendar days of completing the initial IT security training, the Contractor must notify the COR in writing that its employees, in performance of the contract, have completed the training. The COR will inform the Contractor of any other training requirements.

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

(i) Contractor employees must report all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIOHELPDESK@usaid.gov, (202) 712-1234, regardless of day or time, as well as the Contractor Facilities Security Officer. When notifying the USAID Service Desk, Contractor employees must notify, in writing, the Contracting Officer and Bureau for Management, Office of the Chief Information Officer Incident Management Team (M/CIO) at CSIRT@usaid.gov. Contractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, Contractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

ii. The Contractor must provide any supplementary information or reports related to a previously reported incident directly to *CSIRT@usaid.gov* upon request. Correspondence must include related ticket number(s) as provided by the USAID Service Desk with the subject line "Action Required: Potential Security Incident".

(2) Privacy Incident Reporting Requirements: USAID must manage in accordance with Federal laws and regulations the information it collects, uses, maintains, and disseminates in support of its mission and business functions. Any unauthorized use, disclosure, or loss of such information can result in the loss of the public's trust and confidence in the Agency's ability to protect it properly. PII breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. Therefore, incidents involving a breach of PII have a critical time-period for reporting.
Contractor and Contractor staff must report immediately upon discovery all potential and actual privacy breaches to the Contracting Officer, the USAID Service Desk at 202-712-1234 or *CIO-HELPDESK@usaid.gov* , and the Privacy Office at *privacy@usaid.gov* , regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred. The subject line shall read "Action Required: Potential Privacy Incident".

(3) Incident Response Requirements
(i.) All determinations related to Information Security and Privacy Incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by authorized USAID officials at USAID's discretion.

(ii.) The Contractor and Contractor employees must provide full access and cooperation for all activities determined by USAID to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of

Information Security and Privacy Incidents.

(iii.) Incident Response activities required by USAID may include but are not limited to, inspections; investigations; forensic reviews; data analyses and processing; and final determinations of responsibility for the Incident and/or liability for any additional Response activities.

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

(v.) When an incident is determined to be caused by the Contractor or the Contractor's employees through neglect or purposeful conduct, the Contractor must be responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by USAID, whether incurred by USAID, agents under contract or on assignment to USAID, or by third party firms.

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

(g) The Contractor is required to include the substance of this provision in any subcontracts that require the subcontractor, subcontractor employee, or consultant to design, development, or operation of a System of Records on individuals to accomplish an agency function.

In altering this special contract requirement, require subcontractors to report information security and privacy incidents directly to at the USAID Service Desk at 202-712-1234 or *CIOHELPDESK@usaid.gov* / and the Privacy Office at *privacy@usaid.gov*. A copy of the correspondence shall be sent to the prime Contractor(or higher tier subcontractor) and the Contracting Officer referencing the ticket number.

23. SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APRIL 2018)

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 SarbanesOxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

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

(1) HSPD-12 Compliance

Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.
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
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.
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.
Applications designed for normal end users must run in the standard user context without elevated system administration privileges.

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.

i. 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.

ii. 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
(1) Contractor System Oversight/Compliance
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.

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. +--------
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.

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.

(2) 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 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

(3) 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.

24. SEXUAL MISCONDUCT (DECEMBER 2020)

(a) USAID has a zero-tolerance policy for sexual misconduct with the goal of fostering a respectful, safe, healthy and inclusive work environment. USAID maintains policies and procedures to establish a workplace free of sexual misconduct as described in agency policy at ADS Chapter 113, Preventing and Addressing Sexual Misconduct.

(b) USAID has developed two methods for receiving allegations of sexual misconduct: USAID's Unified Misconduct Reporting Portal, available on Launchpad (launchpad.usaid.gov), and Service Desk, phone, (202) 712-1234. These are also available to the Contractor or its employee(s).

(c) USAID may conduct administrative inquiries into allegations of sexual misconduct that occur within U.S. Government facilities or while the contractor employee is performing services under the contract.

The Contracting Officer will provide the results of any inquiry involving a contractor employee to the contractor, subject to federal law and USAID's information disclosure policies. USAID retains the right to suspend or terminate a contractor employee's access to any systems and/or facilities for incidents of sexual misconduct.

(d) The Contractor agrees to incorporate the substance of paragraphs (a) through (d) of this requirement in all subcontracts that may require contractor employees to have routine physical access to USAID facilities.

[END OF SPECIAL CONTRACTING REQUIREMENTS]

CONTRACT CLAUSES

The Contractor will be bound by the terms and conditions of its GSA Multiple Award Schedule (MAS) contract No. 47QRAA23D003U in addition to any terms in this section.

1. FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This Task Order Agreement incorporates all the clauses in GSA Professional Services Schedule contract Number [to be completed at time of award] 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/these address (es): *http://www.arnet.gov/far* *http://www.usaid.gov*.

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 FAR § 52.252-2 for an internet address (if specified) for electronic access to the full text of a clause.

FAR: https://www.acquisition.gov/far/
AIDAR: https://www.usaid.gov/ads/policy/300/aidar

CLAUSES INCORPORATED BY REFERENCE in the GSA Schedule contract.

See https://acquisition.gov/browse/index/far for electronic access to the full text of a clause.

NUMBER	TITLE	DATE
	Federal Acquisition Regulation (48 CFR Chapter 1)	
52.204-7	SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.204-27	PROHIBITION ON A BYTEDANCE COVERED APPLICATION	JUNE 2023
52.222-56	CERTIFICATION REGARDING TRAFFICKING IN PERSONS COMPLIANCE PLAN	OCT 2020
52.252-1	SOLICITATION PROVISIONS INCORPORATED BY REFERENCE	
52.202-1	Definitions	JUN 2020
52-203-5	Covenant Against Contingent Fees	MAY 2014
52-203-7	Anti-Kickback Procedures	JUN 2020
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	JUN 2020
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2019
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.	NOV 2021
52.222-50	Combating Trafficking in Persons.	NOV 2021
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving.	JUNE 2020
52.232-39	Unenforceability of Unauthorized Obligations.	JUNE 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors.	MAR 2023
52.233-3	Protest after Award.	AUG 1996
52.233-3_	Alternate I	JUNE 1985

52.233-4	Applicable Law for Breach of Contract Claim.	OCT 2004
52.243-3	Changes-Time-and-Materials or Labor-Hours.	SEP 2000
52.244-6	Subcontracts for Commercial Products and Commercial Services.	MAR 2023
52.203-3	Gratuities.	APR 1984
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.	JUNE 2020
52.203-13	Contractor Code of Business Ethics and Conduct.	NOV 2021
52.203-15	Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009.	JUNE 2010
52.203-16	Preventing Personal Conflicts of Interest.	JUNE 2020
52.204-1	Approval of Contract.	DEC 1989
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper.	MAY 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards.	JUNE 2020
52.204-6	Unique Entity Identifier	OCT 2016
52.204-13	System for Award Management Maintenance.	OCT 2018
52.204-14	Service Contract Reporting Requirements.	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance.	AUG 2020
52.204-21	Basic Safeguarding of Covered Contractor Information Systems.	NOV 2021
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment.	NOV 2021
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.	NOV 2021
52.215-2	Audit and Records-Negotiation.	JUNE 2020
52.215-2_	Alternate I	MAR 2009
52.215-2_	Alternate II	AUG 2016
52.215-2_	Alternate III	JUNE 1999
52.215-8	Order of Precedence-Uniform Contract Format.	OCT 1997
52.215-10	Price Reduction for Defective Certified Cost or Pricing Data.	AUG 2011
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data-Modifications.	JUNE 2020
52.215-12	Subcontractor Certified Cost or Pricing Data.	JUNE 2020
52.215-13	Subcontractor Certified Cost or Pricing Data-Modifications.	JUNE 2020
52.215-13_	Alternate I	AUG 2020
52.215-19	Notification of Ownership Changes.	OCT 1997
52.216-7	Allowable Cost and Payment.	AUG 2018
52.225-13	Restrictions on Certain Foreign Purchases	FEB 2021

AIDAR 48 CFR Chapter 7

752.202-1	Definitions	JAN 1990
752.204-2	Security Requirements	FEB 1999
752.222-70	USAID Disability Policy	DEC 2004
752.222-71	Nondiscrimination	JUN 2012
752.225-70	Source and Nationality Requirements	FEB 2012
752.245-70	Government Property-USAID Reporting Requirements	OCT 2017
752.7006	Notices	APR 1984
752.7025	Approvals	APR 1984
752.7033	Physical Fitness	JUL 1997

752.7035	Public Notices	DEC 1991
752.7037	Child Safeguarding Standards	AUG 2016
752.7038	Nondiscrimination against End-Users of Supplies or Services of Supplies or Services	OCT 2016

I.1 FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)

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

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition*.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the

covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services.

I.2 CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (APR 2014) (DEVIATION M-OAA-DEV-FAR-18-1C)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C.

4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section 3.908 of the Federal Acquisition Regulation.

(d) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold.

I.3 FAR 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL 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 Safety Protocols 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, as Amended (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.

Notice Regarding Any Court Order Affecting the Implementation of E.O. 14042

USAID will take no action to enforce the clause (FAR 52.223-99) implementing the requirements of Executive Order 14042, absent further written notice from USAID, where the place of performance identified in the contract is in a U.S. state or outlying area subject to a court order prohibiting the application of requirements pursuant to the Executive Order (hereinafter, "Excluded State or Outlying Area"). In all other circumstances, USAID will enforce the clause, except for contractor employees who perform substantial work on or in connection with a covered contract in an Excluded State or Outlying Area, or in a covered contractor workplace

located in an Excluded State or Outlying Area. A current list of such Excluded States and Outlying Areas is maintained at https://www.saferfederalworkforce.gov/contractors/.

I.4 FAR 52.204-27 PROHIBITION ON A BYTEDANCE COVERED APPLICATION (JUN 2023)

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

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) 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 support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(b) *Prohibition*. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on executive agency information technology, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the Contracting Officer provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

[END OF SECTION I]