SECTION D - BRANDING 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 Standard Graphic Identity". 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

The Contractor shall 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 http://www.usaid.gov/policy/ads/300/320.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/Basic Education 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 sub-Contractors' corporate identities or logos must not be used on USAID-funded program materials.

D.3 MARKING AND BRANDING STRATEGY

Anticipated elements of marking plan: Deliverables to be marked, include products, equipment and inputs delivered; places where program activities are carried out; external public communications, studies, reports, publications and informative and promotional products; and workshops, conferences, fairs, media related activities and any such events. Publications authored by Contractors or other non-USAID employees must include the following disclaimer on the title page: "The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government." Threats and restrictions to the security of the program need to be identified and assessed in order to request any necessary exception from the marking requirement in accordance with ADS 320.3.2.

USAID's web page contains the electronic version of the Graphic Standards Manual that is compulsory for all Contractors. Marking under this contract shall comply with the "USAID Graphics Standards Manual" available at http://www.usaid.gov/branding/acquisition.html.

The Contractor's Branding Implementation Plan (BIP) and Marking Plan will be approved separately.

D.4 FEED THE FUTURE TRADEMARKING AND BRANDING

Per ADS 320.3.4, a special determination signed by the USAID Administrator in December 2014 authorized the Feed the Future initiative to issue its own naming, marking and branding guidance for use by USAID and its implementing partners. It is the first (and currently only) Presidential Initiative to receive this exception.

Per this determination, USAID contracts, grants and cooperative agreements awarded on or after January 1, 2015, which are funded by the USG's Feed the Future initiative must include the Feed the Future logo in addition to USAID's identity on communication products. The Contractor is required to comply (and ensure compliance by partners) with USAID's branding and marking requirements set forth in 2 CFR 700.16 with Feed the Future specific guidance located at feedthefuture.gov.

[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 http://acquisition.gov/far/index.html for electronic access to the full text of a clause

NUMBER	TITTLE	DATE
52.246-5	INSPECTION OF SERVICES – COST REIMBURSEMENT	APR 1984

[END OF SECTION E]

SECTION F - DELIVERIES OR PERFORMANCE

F.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 with the same force and effect as if they were given in full text. See http://acquisition.gov/far/index.html for electronic access to the full text of a clause.

NUMBER	TITLE	DATE
52.242-15	STOP-WORK ORDER	AUG 1989
52.242-15	ALTERNATE I	APR 1984

F.2 AUTHORIZED WORKDAY / WEEK

No overtime or premium pay is authorized under this Contract. The Contractor is authorized up to a 6-day workweek (8 hours per day) for all short-term consultants to maximize work time while in Bangladesh. All long-term employees under the activity should follow a standard workweek in accordance with local laws and the Contractor's policies as applicable. Any other authorization for an extended workday/week for personnel will need to be requested in advance from the COR. The Contractor's field staff must keep the same operating schedule as the US Embassy in Bangladesh.

[END OF SECTION F]

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this solicitation is 937, which is the

United States, the recipient country, and developing countries other than advanced developing countries, but excluding any country that is a prohibited source.

A list of developing countries is available at: http://www.usaid.gov/sites/default/files/documents/1876/310maa.pdf

A list of advanced developing countries is available at:
http://www.usaid.gov/sites/default/files/documents/1876/310mab.pdf

H.2 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.

H.3 INTERNATIONAL TRAVEL APPROVAL

All international air travel must be in accordance with AIDAR 752.7032, International Travel Approval and Notification Requirements, and AIDAR 752.7027, Personnel; comply with the terms and conditions of the Contract; and, is subject to availability of funds.

All international air travel funded under this contract, as delegated by the CO, will be approved separately by the designated COR.

H.4 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 CO.

H.5 EXECUTIVE ORDER ON TERRORISM FINANCING (FEB 2002)

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 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.

H.6 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.7 CLOUD COMPUTING (APRIL 2018)

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

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

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

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

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

“Spillage” means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited,(i.e., authorized) for the applicable security level of the data or information. “Cloud Service Provider” or CSP means a company or organization that offers some component of cloud computing –typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

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

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

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term “individual” refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

(b) Applicability

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

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

(1) The Contractor shall not access, use, or disclose 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, Federal information shall only be for purposes specified in this contract.
ii. The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.
iii. These access, use, and disclosure prohibitions and obligations shall remain effective beyond the expiration or termination of this contract.
(2) The Contractor shall use related Federal information only to manage the operational environment that supports the Federal information and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) Records Management and Access to Information

(1) The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with capabilities such as those identified in the provisions of this contract and National Archives and Records Administration (NARA) retention policies.
(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Federal information , including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by the Contracting Officer in support of government compliance requirements to include but not limited to Freedom of Information Act, Privacy Act, e-Discovery, e- Records and legal or security investigations.
(3) The Contractor shall retain and maintain all Federal information in accordance with records retention provisions negotiated by the terms of the contract and in accordance with USAID records retention policies.
(4) The Contractor shall dispose of Federal information in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

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

(f) Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Contractor's discovery of a spillage or security incident involving classified information, the Contractor shall immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or information security incident in compliance with agency-specific instructions. The Contractor will also notify the Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer. The Contractor will abide by USAID instructions on correcting such a spill or information security incident. For all spills and information security incidents involving unclassified and/or SBU information, the protocols outlined above in section (g) and (h) below shall apply.
(g) Information Security Incidents
(1) Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the information security incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.
(i)Contractor employees must report via e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: 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.

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.

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

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

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

(j) Security Requirements:

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

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

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

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

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

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

(7) The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements and to allow for appropriate risk decisions for an

Information Technology security program. The Government reserves the right to conduct onsite inspections. The Contractor must make appropriate personnel available for interviews and provide all necessary documentation during this review and as necessary for continuous monitoring activities.
(k) Privacy Requirements: Cloud Service Provider (CSP) must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect Personally Identifiable Information (PII) about individuals that will be collected and maintained by the Contractor solution. The Contractor responsibilities include full cooperation for any request for disclosure, subpoena, or other judicial process seeking access to records subject to the Privacy Act of 1974.

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

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

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have beenresolved or mitigated. Additionally, at USAID's request, the Contractor must submit reports or provide a dashboardwhere 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 inaccordance 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.8 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) andthe 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.

H.9 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.

H.18 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JULY 2007)

(a) Before a Contractor (or a Contractor's employee) may obtain a USAID ID (new or replacement) authorizing him/her routine access to USAID facilities, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form and a passport size photo. One identity source document must be a valid Federal or state government-issued picture ID. (Overseas foreign nationals must comply with the requirements of the Regional Security

Office.) USAID/Washington Contractors must contact the USAID Security Office to obtain the list of acceptable forms of documentation, and Contractors working in overseas Missions must obtain the acceptable documentation list from the Regional Security Officer. Submission of these documents, and related background checks, are mandatory in order for the Contractor to receive a building access ID, and before access will be granted to any of USAID's information systems. All Contractors must physically present these two source documents for identity proofing at their USAID/Washington or Mission Security Briefing. The Contractor or his/her Facilities Security Officer must return any issued building access ID and remote authentication token to USAID custody upon termination of the individual's employment with the Contractor or completion of the contract, whichever occurs first.

(b) The Contractor must comply with all applicable HSPD-12 and PIV procedures, as described above, and any subsequent USAID or government-wide HSPD-12 and PIV procedures/policies, including any subsequent related USAID General Notices, Office of Security Directives and/or Automated Directives System (ADS) policy directives and required procedures. This includes HSPD-12 procedures established in USAID/Washington and those procedures established by the overseas Regional Security Office.

(c) The Contractor is required to include this provision in any subcontracts that require the sub-contractor or sub-contractor employee to have routine physical access to USAID space or logical access to USAID's information systems.

H.23 AIDAR 752.231-71 SALARY SUPPLEMENTS FOR HOST GOVERNMENT (HG) EMPLOYEES (MAR 2015) (a) Salary supplements are payments made that augment an employee's base salary or premiums, overtime, extra payments, incentive payment and allowances for which the HG employee would qualify under HG rules or practice for the performance of his/hers regular duties or work performed during his/hers regular office hours. Per diem, invitational travel, honoraria and payment for work carried out outside of normal working hours are not considered to be salary supplements.

(b) Salary supplements to HG Employees are not allowable without the written approval of the Contracting Officer.

(c) The Contractor must insert a clause containing all the terms of this clause, including the requirement to obtain the written approval of the contracting officer for all salary supplements, in all subcontracts under this contract that may entail HG employee salary supplements.

H.24 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.

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.35 FAR 52.204-27 PROHIBITION ON A BYTEDANCE COVERED APPLICATION NO TIKTOK ON GOVERNMENT DEVICES (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 H]

PART II - CONTRACT CLAUSES
SECTION I - CONTRACT CLAUSES

I.1 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/these address(es):

FAR: http://acquisition.gov/far/index.html

NUMBER	TITLE	DATE
52.202-1	DEFINITIONS	JUN 2020
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	JUN 2020
52.203-7	ANTI-KICKBACK PROCEDURES	JUN 2020
52.203-8	CANCELLATION, RESCISSION AND RECOVERY OF FUNDS FOR ILLEGAL 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	JUN 2020
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	JUN 2020
52.203-16	PREVENTING PERSONAL CONFLICTS OF INTEREST	JUN 2020
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	JUN 2020
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER	MAY 2011
52.204-19	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS	DEC 2014

52.204-21	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS	JUN 2016
52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES	JUL 2018
52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT	AUG 2020
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	JUN 2020
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	JUN 2020
52.215-2	AUDIT AND RECORDS—NEGOTIATION	JUN 2020
52.215-14	INTEGRITY OF UNIT PRICES	JUN 2020
52.215-19	NOTIFICATION OF OWNERSHIP CHANGES	OCT 1997
52.215-23	LIMITATIONS ON PASS-THROUGH CHARGES	JUN 2020
52.216-7	ALLOWABLE COST AND PAYMENT	AUG 2018
52.217-2	CANCELLATION UNDER MULTI-YEAR CONTRACTS	OCT 1997
52.217-8	OPTION TO EXTEND SERVICES	NOV 1999
52.222-3	CONVICT LABOR	JUN 2003
52.222-17	NONDISPLACEMENT OF QUALIFIED WORKERS	MAY 2014
52.222-19	CHILD LABOR—COOPERATION WITH AUTHORITIES AND REMEDIES	JAN 2020
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
52.222-35	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
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	OCT 2015
52.223-6	DRUG FREE WORKPLACE	MAY 2001
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	JUN 2020
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	FEB 2021
52.227-3	PATENT INDEMNITY	APR 1984
52.227-13	PATENT RIGHTS—OWNERSHIP BY THE GOVERNMENT	DEC 2007
52.227-14	RIGHTS IN DATA—GENERAL	MAY 2014
52.228-7	INSURANCE—LIABILITY TO THIRD PERSONS	MAR 1996
52.228-8	LIABILITY AND INSURANCE—LEASED MOTOR VEHICLES	MAY 1999
52.229-8	TAXES—FOREIGN COST-REIMBURSEMENT CONTRACTS	MAR 1990
52.230-2	COST ACCOUNTING STANDARDS	JUN 2020
52.230-6	ADMINISTRATION OF COST ACCOUNTING STANDARDS	JUN 2010
52.232-1	PAYMENTS	APR 1984
52.232-9	LIMITATION ON WITHHOLDING OF PAYMENTS	APR 1984
52.232-17	INTEREST	MAY 2014
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.232-23	ASSIGNMENT OF CLAIMS	MAY 2014
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.233-1	DISPUTES	MAY 2014
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.236-5	MATERIALS AND WORKMANSHIP	APR 1984
52.236-7	PERMITS AND RESPONSIBILITIES	NOV 1991
52.236-18	WORK OVERSIGHT IN COST-REIMBURSEMENT CONSTRUCTION CONTRACTS	APR 1984
52.236-19	ORGANIZATION AND DIRECTION OF THE WORK	APR 1984
52.237-3	CONTINUITY OF SERVICES	JAN 1991
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
52.242-13	BANKRUPTCY	JUL 1995
52.243-2	CHANGES—COST-REIMBURSEMENT ALTERNATE I	APR 1984

52.245-1	GOVERNMENT PROPERTY	JAN 2017
52.245-9	USE AND CHARGES	APR 2012
52.246-23	LIMITATION OF LIABILITY	FEB 1997
52.246-25	LIMITATION OF LIABILITY—SERVICES	FEB 1997
52.249-6	TERMINATION (COST REIMBURSEMENT)	MAY 2004
52.249-14	EXCUSABLE DELAYS	APR 1984
52.253-1	COMPUTER GENERATED FORMS	JAN 1991

I.2 AIDAR 752.252-2 AIDAR CLAUSES INCORPORATED BY REFERENCE (MAR 2015)

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 all AIDAR solicitation provisions and contract clause is contained in the Code of Federal Regulations (CFR) located at 48 CFR chapter 7, and at the following Web address:
http://www.usaid.gov/sites/default/files/documents/1868/aidar_0.pdf

NUMBER	TITLE	DATE
752.202-1	DEFINITIONS	
	ALTERNATE 70	JAN 1990
	ALTERNATE 72	JUN 2009
752.204-2	SECURITY REQUIREMENTS	FEB 1999
752.209-71	ORGANIZATIONAL CONFLICTS OF INTEREST DISCOVERED AFTER AWARD	JUN 1993
752.211-70	LANGUAGE AND MEASUREMENT	JUN 1992
752.219-70	USAID MENTOR-PROTÉGÉ PROGRAM	JUL 2007
752.222-71	NONDISCRIMINATION	JUN 2012
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
752.236-70	STANDARDS FOR ACCESSIBILITY FOR THE DISABLED IN USAID CONSTRUCTION CONTRACTS	JUL 2007
752.242-70	PERIODIC PROGRESS REPORTS	OCT 2007
752.245-70	GOVERNMENT PROPERTY – USAID REPORTING REQUIREMENTS	OCT 2017
752.245-71	TITLE TO AND CARE OF PROPERTY	APR 1984
752.7002	TRAVEL AND TRANSPORTATION	JAN 1990
752.7004	EMERGENCY LOCATOR INFORMATION	JUL 1997
752.7006	NOTICES	APR 1984
752.7008	USE OF GOVERNMENT FACILITIES OR PERSONNEL	APR 1984
752.7009	MARKING	JAN 1993
752.7010	CONVERSION OF U.S. DOLLARS TO LOCAL CURRENCY	APR 1984
752.7013	CONTRACTOR-MISSION RELATIONSHIPS	OCT 1989
	DEVIATION	JUN 2020
752.7015	USE OF POUCH FACILITIES	JUL 1997
752.7019	PARTICIPANT TRAINING	JAN 1999
752.7025	APPROVALS	APR 1984
752.7027	PERSONNEL	DEC 1990
752.7032	INTERNATIONAL TRAVEL APPROVAL AND NOTIFICATION REQUIREMENTS	APR 2014
752.7033	PHYSICAL FITNESS	JUL 1997
752.7035	PUBLIC NOTICES	DEC 1991
752.7036	USAID IMPLEMENTING PARTNER NOTICES (IPN) PORTAL FOR ACQUISITION	JUL 2014
752.7038	NONDISCRIMINATION AGAINST END-USERS OF SUPPLIES OR SERVICES	OCT 2016

I.3 FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(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–

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

(c) 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);

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

(e) 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–

(f) 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;

(g) 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-

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

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

(j) 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);

(k) 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);

(l) 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

(m) 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.

(n) 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.

(o) 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.

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

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

(r) 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.

(s) 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.

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

(u) 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.

(v) 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.

(w) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph I and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

I.4 FAR 52.227-23 RIGHTS TO PROPOSAL DATA (TECHNICAL) (JUN 1987)

Except for data contained on pages (n/a), it is agreed that as a condition of award of this contract, and notwithstanding the conditions of any notice appearing thereon, the Government shall have unlimited rights (as defined in the "Rights in Data–General" clause contained in this contract) in and to the technical data contained in the proposal dated_____upon which this contract is based.

I.5 AIDAR 752.229-71 REPORTING OF FOREIGN TAXES (JUL 2007)

a) The contractor must annually submit a report by April 16 of the next year.
b) Contents of report. The report must contain:
   1) Contractor name.
   2) Contact name with phone, fax number and email address.
   3) Contract number(s).
   4) Amount of foreign taxes assessed by a foreign government [each foreign government must be listed 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 are to be reported. Foreign taxes by a third party foreign government are not to be reported. For example, if a contractor performing in Lesotho using foreign assistance funds should purchase commodities in South Africa, any taxes imposed by South Africa would not be included in the report for Lesotho (or South Africa).
   6) Any reimbursements received by the contractor during the period in paragraph (b)(4) of this clause regardless of when the foreign tax was assessed and any reimbursements on the taxes reported in paragraph (b)(4) of this clause received through March 31.
   7) Report is required even if the contractor did not pay any taxes during the reporting period.
   8) Cumulative reports may be provided if the contractor is implementing more than one program in a foreign country.
c) Definitions. As used in 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 customs duties assessed by a foreign government on a commodity. It does not include foreign sales taxes.
d) Where. Submit the reports at dhakafinancialanalysis@usaid.gov

e) Subagreements. The contractor must include this reporting requirement in all applicable subcontracts and other subagreements.

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

I.6 AIDAR 752.7101 VOLUNTARY POPULATION PLANNING ACTIVITIES (JUNE 2008)

a) *Requirements for Voluntary Sterilization Program*. None of the funds made available under this Contract shall be used to pay for the performance of involuntary sterilization as a method of family planning or to coerce or provide any financial incentive to any individual to practice sterilization.

b) Prohibition on Abortion-Related Activities.
1) No funds made available under this Contract will be used to finance, support, or be attributed to the following activities: (i) procurement or distribution of equipment intended to be used for the purpose of inducing abortions as a method of family planning; (ii) special fees or incentives to any person to coerce or motivate them to have abortions; (iii) payments to persons to perform abortions or to solicit persons to undergo abortions; (iv) information, education, training, or communication programs that seek to promote abortion as a method of family Planning ; and (v) lobbying for or against abortion. The term "motivate", as it relates to family planning assistance, shall not be construed to prohibit the provision, consistent with local law, of information or counseling about all pregnancy options.
2) No funds made available under this Contract will be used to pay for any biomedical research which relates, in whole or in part, to methods of, or the performance of, abortions or involuntary sterilizations as a means of family planning. Epidemiologic or descriptive research to assess the incidence, extent or consequences of

abortions is not precluded.

c) The Contractor shall insert this provision in all subcontracts.

I.7 AIDAR 752.7037 CHILD SAFEGUARDING STANDARDS (AUG 2016)

(a) Implementation of activities under this award may involve children, or personnel engaged in the implementation of the award may come into contact with children, which could raise the risk of child abuse, exploitation, or neglect within this award. The contractor agrees to abide by the following child safeguarding core principles:
   (1) Ensure compliance with host country and local child welfare and protection legislation or international standards, whichever gives greater protection, and with U.S. law where applicable;
   (2) Prohibit all personnel from engaging in child abuse, exploitation, or neglect;
   (3) Consider child safeguarding in project planning and implementation to determine potential risks to children that are associated with project activities and operations;
   (4) Apply measures to reduce the risk of child abuse, exploitation, or neglect, including, but not limited to, limiting unsupervised interactions with children; prohibiting exposure to pornography; and complying with applicable laws, regulations, or customs regarding the photographing, filming, or other image generating activities of children;
   (5) Promote child-safe screening procedures for personnel, particularly personnel whose work brings them in direct contact with children; and
   (6) Have a procedure for ensuring that personnel and others recognize child abuse, exploitation, or neglect; mandating that personnel and others report allegations; investigating and managing allegations; and taking appropriate action in response to such allegations, including, but not limited to, dismissal of personnel.

(b) The contractor must also include in the code of conduct for all personnel implementing USAID-funded activities, the child safeguarding principles in paragraphs (a)(1) through (6) of this clause.

(c) The following definitions apply for purposes of this clause:
   (1) Child. A child or children are defined as persons who have not attained 18 years of age.
   (2) Child abuse, exploitation, or neglect. Constitutes any form of physical abuse; emotional ill-treatment; sexual abuse; neglect or insufficient supervision; trafficking; or commercial, transactional, labor, or other exploitation resulting in actual or potential harm to the child's health, well-being, survival, development, or dignity. It includes, but is not limited to: Any act or failure to act which results in death, serious physical or emotional harm to a child, or an act or failure to act which presents an imminent risk of serious harm to a child.
   (3) Emotional abuse or ill treatment. Constitutes injury to the psychological capacity or emotional stability of the child caused by acts, threats of acts, or coercive tactics. Emotional abuse may include, but is not limited to: Humiliation, control, isolation, withholding of information, or any other deliberate activity that makes the child feel diminished or embarrassed.
   (4) Exploitation. Constitutes the abuse of a child where some form of remuneration is involved or whereby the perpetrators benefit in some manner. Exploitation represents a form of coercion and violence that is detrimental to the child's physical or mental health, development, education, or well-being.
   (5) Neglect. Constitutes failure to provide for a child's basic needs within USAID funded activities that are responsible for the care of a child in the absence of the child's parent or guardian.
   (6) Physical abuse. Constitutes acts or failures to act resulting in injury (not necessarily visible), unnecessary or unjustified pain or suffering without causing injury, harm or risk of harm to a child's health or welfare, or death. Such acts may include, but are not limited to: Punching, beating, kicking, biting, shaking, throwing, stabbing, choking, or hitting (regardless of object used), or burning. These acts are considered abuse regardless of whether they were intended to hurt the child.
   (7) Sexual abuse. Constitutes fondling a child's genitals, penetration, incest, rape, sodomy, indecent exposure, and exploitation through prostitution or the production of pornographic materials.

(d) The contractor must insert this clause in all subcontracts under this award.

[END OF SECTION I]