# ATTACHMENT C
# Prime Contract General Provisions

The Subcontractor agrees to comply with all applicable requirements, specifications, and conditions of the Prime Contract to the extent to which they are incorporated into this Subcontract Agreement. Any applicable requirements, specifications, and conditions of the Prime Contract, specified by law, are included in this Subcontract Agreement. The clauses in FAR Subpart 52.2 and AIDAR Subpart 752 referenced in the Prime Contract are required to be flowed down to subcontractors, in effect on the date of this Subcontract. In this section, clauses from Section I – Prime Contract General Requirements – are herein incorporated by reference and are listed below. In addition, other clauses are listed in full text. Whether a clause appears as incorporated by reference or as full text, it applies to this Subcontract Agreement. Unless a current version of a clause is specifically incorporated in the body of this Subcontract, to the extent that an earlier version of any such clause is included in the Prime Contract under which this Subcontract is issued, the date of the clause as it appears in such Prime Contract shall be controlling and said version shall be incorporated herein.

In all such clauses, the term "Contractor" shall mean the Subcontractor performing under this Subcontract, the term "Contract" shall mean this Subcontract, and the terms "Government", "Contracting Officer" and equivalent phrases shall mean the Contractor and the DAI Contractual Representative, respectively. It is intended that the referenced clauses shall apply to the Subcontractor in such manner as is necessary to reflect the position of the Subcontractor as a subcontractor to the Prime Contractor, to insure the Subcontractor's obligations to the Prime Contractor and to the U.S. Government, and to enable the Prime Contractor to meet its obligations under its Prime Contract. Clauses not requiring flow down from the Contractor to the Subcontractor, but nevertheless specified herein shall have full force and effect in performance of this Subcontract.

**Clauses Incorporated by Reference**

This Subcontract incorporates one or more of the following clauses by reference, suitably modified to properly identify the parties, with same force and effect as if they were given in full text. The complete text will be made available to Subcontractor upon request. The full text may also be accessed electronically at the following website: http://www.arnet.gov/far/

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.

## 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):

- https://www.acquisition.gov/
- https://www.usaid.gov/sites/default/files/documents/1868/aidar_0.pdf

**Federal Acquisition Regulation Clauses:**

| NUMBER | TITLE | DATE |
|---|---|---|
| 52.202-1 | Definitions | (NOV 2013) |
| 52.203-3 | Gratuities | (APR 1984) |

| | | |
|---|---|---|
| 52.203-5 | Covenant Against Contingent Fees | (MAY 2014) |
| 52.203-6 | strictions on Subcontractor Sales to the Government | (SEP 2006) |
| 52.203-7 | Anti-Kickback Procedures | (MAY 2014) |
| 52.203-8 | Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity | (MAY 2014) |
| 52.203-10 | Price or Fee Adjustment for Illegal or Improper Activity | (MAY 2014) |
| 52.203-12 | Limitation on Payments to Influence Certain Federal Transactions | (OCT 2010) |
| 52.203-13 | Contractor Code of Business Ethics and Conduct | (OCT 2015) |
| 52.203-14 | Display Of Hotline Poster(s) | (OCT 2015) |
| 52.203-16 | Preventing Personal Conflicts of Interest | (DEC 2011) |
| 52.203-17 | Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights | (APR 2014) |
| 52.204-2 | Security Requirements | (AUG 1996) |
| 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 | (OCT 2016) |
| 52.204-14 | Service Contract Reporting Requirements | (OCT 2016) |
| 52.204-19 | Incorporation by Reference of Representations and Certifications | (DEC 2014) |
| 52.209-6 | Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment | (OCT 2015) |
| 52.209-10 | Prohibition on Contracting With Inverted Domestic Corporations | (NOV 2015) |
| 52.210-1 | Market Research | (APR 2011) |
| 52.215-2 | Audit and Records - Negotiation | (OCT 2010) |
| 52.215-8 | Order of Precedence - Uniform Contract Format | (OCT 1997) |
| 52.215-14 | Integrity of Unit Prices | (OCT 2010) |
| 52.215-17 | Waiver of Facilities Capital Cost of Money | (OCT 1997) |
| 52.215-23 | Limitations on Pass-Through Charges | (OCT 2009) |
| 52.215-23 | Limitations on Pass-Through Charges (OCT 2009) -- Alternate I | (OCT 2009) |

| | | |
|---|---|---|
| 52.222-3 | Convict Labor | (JUN 2003) |
| 52.222-17 | Nondisplacement of Qualified Workers | (MAY 2014) |
| 52.222-20 | Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000 | (MAY 2014) |
| 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) |
| 52.222-2 | Payment For Overtime Premiums | (JUL 1990) |
| 52.222-37 | Employment Reports on Veterans | (FEB 2016) |
| 52.222-40 | Notification of Employee Rights Under the National Labor Relations Act | (DEC 2010) |
| 52.222-41 | Service Contract Labor Standards | (MAY 2014) |
| 52.222-50 | Combating Trafficking in Persons | (MAR 2015) |
| 52.222-54 | Employment Eligibility Verification | (OCT 2015) |
| 52.222-55 | Minimum Wages Under Executive Order 13658 | (DEC 2015) |
| 52.222-62 | Paid Sick Leave Under Executive Order 13706 | (JAN 2017) |
| 52.223-6 | Drug-Free Workplace | (MAY 2001) |
| 52.223-18 | Encouraging Contractor Policies to Ban Text Messaging While Driving | (AUG 2011) |

| | | |
|---|---|---|
| 52.225-13 | Restrictions on Certain Foreign Purchases | (JUN 2008) |
| 52.225-14 | Inconsistency between English Version and Translation of Contract | (FEB 2000) |
| 52.225-19 | Contractor Personnel In A Designated Operational Area Or Supporting A Diplomatic Or Consular Mission Outside The United States | (MAR 2008) |
| 52.227-3 | Patent Indemnity | (APR 1984) |
| | Alternate I | (APR 1984) |
| | Alternate II | (APR 1984) |
| 52.227-14 | Rights in Data-General | (MAY 2014) |
| 52.227-17 | Rights in Data--Special Works | (DEC 2007) |
| 52.228-3 | Workers' Compensation Insurance (Defense Base Act) | (JUL 2014) |
| 52.228-7 | Insurance - Liability to Third Persons | (MAR 1996) |
| 52.229-8 | Taxes - Foreign Cost-Reimbursement Contracts | (MAR 1990) |
| 52.230-6 | Administration of Cost Accounting Standards | (JUN 2010) |
| 52.232-17 | Interest | (MAY 2014) |
| 52.232-23 | Assignment of Claims | (MAY 2014) |
| | Alternate I | (APR 1984) |
| 52.232-25 | Prompt Payment | (JAN 2017) |
| | Alternate I | (FEB 2002) |
| 52.232-33 | Payment by Electronic Funds Transfer - System for Award Management | (JUL 2013) |
| 52.232-39 | Unenforceability of Unauthorized Obligations | (JUN 2013) |
| 52.232-40 | Providing Accelerated Payments to Small Business Subcontractors | (DEC 2013) |
| 52.233-1 | Disputes | (MAY 2014) |
| | Alternate I | (DEC 1991) |
| 52.233-3 | Protest after Award. (AUG 1996) - Alternate I | (JUN 1985) |
| 52.233-4 | Applicable Law for Breach of Contract Claim | (OCT 2004) |
| 52.239-1 | Privacy or Security Safeguards | (AUG 1996) |
| 52.242-1 | Notice of Intent to Disallow Costs | (APR 1984) |
| 52.242-3 | Penalties for Unallowable Costs | (MAY 2014) |
| 52.242-13 | Bankruptcy | (JUL 1995) |
| 52.243-7 | Notification Of Changes | (JAN 2017) |
| 52.244-2 | Subcontracts | (OCT 2010) |
| | Alternate I | (JUN 2007) |
| 52.244-5 | Competition in Subcontracting | (DEC 1996) |
| 52.244-6 | Subcontracts For Commercial Items | (JAN 2017) |
| 52.245-1 | Government Property | (JAN 2017) |
| 52.245-9 | Use and Charges | (APR 2012) |
| 52.246-25 | Limitation of Liability - Services | (FEB 1997) |
| 52.247-1 | Commercial Bill Of Lading Notations | (FEB 2006) |
| 52.247-63 | Preference for U.S.-Flag Air Carriers | (JUN 2003) |
| 52.249-14 | Excusable Delays | (APR 1984) |

**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.

**U.S. Agency for International Development Acquisition Regulation (AIDAR) 48CFR CHAPTER 7 Clauses:**

| NUMBER | TITLE | DATE |
|---|---|---|
| 752.202-1 | Definitions | (JAN 1990) |
| 752.204-2 | Security Requirements | (FEB 1999) |
| 752.209-71 | Organizational Conflicts of Interest Discovered After Award | (JUN 1993) |
| 752.216-70 | Award Fee | (MAY 1997) |
| 752.225-70 | Source and Nationality Requirements | (FEB 2012) |
| 752.228-3 | Worker's Compensation Insurance (Defense Base Act) | (DEC 1991) |
| 752.228-7 | Insurance - Liability to Third Persons | (JUL 1997) |
| 752.229-70 | Federal, State and Local Taxes | |
| 752.231-72 | Conference Planning and Required Approvals | (AUG 2013) |
| 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) |
| 752.7010 | Conversion of U.S. Dollars to Local Currency | (APR 1984) |
| 752.7011 | Orientation and Language Training | (APR 1984) |
| 752.7013 | Contractor-Mission Relationships | (OCT 1989) |
| 752.7014 | Notice of Changes in Travel Regulations | (JAN 1990) |
| 752.7015 | Use of Pouch Facilities | (JUL 1997) |
| 752.7018 | Health and Accident Coverage for USAID Participant Trainees | (JAN 1999) |
| 752.7019 | Participant Training | (JAN 1999) |
| 752.7023 | Required Visa Form for USAID Participants | (APR 1984) |

| | | |
|---|---|---|
| 752.7029 | Post Privileges | (JUL 1993) |
| 752.7030 | Inspection Trips by Contractor's Officers and Executives | (APR 1984) |
| 752.7031 | Leave and Holidays | (OCT 1989) |
| 752.7032 | International Travel Approval and Notification Requirements | (APR 2014) |
| 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 | (OCT 2016) |

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

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

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

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

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

**I.2 FAR 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)**

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

*Covered contractor information system* means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

*Federal contract information* means information, not intended for public release, that is provided by

or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

*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 system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

*Safeguarding* means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements and procedures*. (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii)Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements*. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

## I.3 FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 days.

## I.4 FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 1 day; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this

option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years.

**I.5 FAR 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (OCT 2015)**

(a) Definitions. As used in this clause-

"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran," and "recently separated veteran" have the meanings given at FAR 22.1301.

(b) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $150,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

**I.6 FAR 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)**

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

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

**I.7 FAR 52.247-67 SUBMISSION OF TRANSPORTATION DOCUMENTS FOR AUDIT (FEB 2006)**

(a) The Contractor shall submit to the address identified below, for prepayment audit, transportation documents on which the United States will assume freight charges that were paid-

(1) By the Contractor under a cost-reimbursement contract; and

(2) By a first-tier subcontractor under a cost-reimbursement subcontract thereunder.

(b) Cost-reimbursement Contractors shall only submit for audit those bills of lading with freight shipment charges exceeding $100. Bills under $100 shall be retained on-site by the Contractor and made available for on-site audits. This exception only applies to freight shipment bills and is not intended to apply to bills and invoices for any other transportation services.

(c) Contractors shall submit the above referenced transportation documents

to- oceantransportation@usaid.gov or ofr@usaid.gov

## I.8 AIDAR 752.225-9 BUY AMERICAN ACT - TRADE AGREEMENTS ACT - BALANCE OF PAYMENTS PROGRAM

The clause prescribed by FAR 25.408(a)(2) is not generally included in USAID contracts when more stringent source requirements are stated in the contract or when inclusion is not appropriate under FAR 25.403, or 725.403 of this chapter. (See Executive Order No. 11223, dated May 12, 1965, 30 FR 6635.) The clause setting forth USAID's source restrictions is shown in section 752.225-70.

## I.9 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 to: [contracting officer must insert address and point of contact at the Embassy, Mission, or CFO/CMP as appropriate].

(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.11 AIDAR 752.7034 ACKNOWLEDGMENT AND DISCLAIMER (DEC 1991)**

(a) USAID shall be prominently acknowledged in all publications, videos or other information/media products funded or partially funded through this contract, and the product shall state that the views expressed by the author(s) do not necessarily reflect those of USAID. Acknowledgments should identify the sponsoring USAID Office and Bureau or Mission as well as the U.S. Agency for International Development substantially as follows: "This [publication, video or other information/media product (specify)] was made possible through support provided by the Office of Private Capital and Microenterprise, Bureau for Economic Growth, Education and Environment, U.S. Agency for International Development, under the terms of Contract No. AID-OAA-C-17-00090. The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of the U.S. Agency for International Development."

(b) Unless the contractor is instructed otherwise by the cognizant technical office publications, videos or other information/media products funded under this contract and intended for general readership or other general use will be marked with the USAID logo and/or U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT appearing either at the top or at the bottom of the front cover or, if more suitable, on the first inside title page for printed products, and in equivalent/appropriate location in videos or other information/media products. Logos and markings of co-sponsors or authorizing institutions should be similarly located and of similar size and appearance.

**I.12 52.204-23 - Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)**

(a) Definitions.
As used in this clause—Covered article means any hardware, software, or service that—

(1) Is developed or provided by a covered entity;
(2) Includes any hardware, software, or service developed or provided in whole in part by a covered entity; or
(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

*Covered entity* means—
(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition.
Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115–91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and
(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.
(c) Reporting requirement.
(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website 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 (c)(1) of this clause:
(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) 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 report pursuant to paragraph (c)(1) 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 a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.
(d) Subcontract
The subcontractor shall insert the substance of this clause, including this paragraph (d) in all subcontract including subcontracts for the acquisition of commercial items."

**[END OF SECTION I]**

**[END OF ATTACHMENT C]**

DAI
Shaping a more livable world.

# ATTACHMENT D
# Prime Contract Special Provisions

The Subcontractor agrees to comply with all applicable requirements, specifications, and conditions of the Prime Contract to the extent to which they are incorporated into this Subcontract Agreement. Any applicable requirements, specifications, and conditions of the Prime Contract, specified by law, are included in this Subcontract Agreement. The clauses in FAR Subpart 52.2 and AIDAR Subpart 752 referenced in the Prime Contract are required to be flowed down to subcontractors, in effect on the date of this Subcontract. In this section, clauses from Section H – Prime Contract Special Requirements – are herein incorporated by reference and are listed below. In addition, other clauses are listed in full text. Whether a clause appears as incorporated by reference or as full text, it applies to this Subcontract Agreement. Unless a current version of a clause is specifically incorporated in the body of this Subcontract, to the extent that an earlier version of any such clause is included in the Prime Contract under which this Subcontract is issued, the date of the clause as it appears in such Prime Contract shall be controlling and said version shall be incorporated herein.

In all such clauses, the term "Contractor" shall mean the Subcontractor performing under this Subcontract, the term "Contract" shall mean this Subcontract, and the terms "Government", "Contracting Officer" and equivalent phrases shall mean the Contractor and the DAI Contractual Representative, respectively. It is intended that the referenced clauses shall apply to the Subcontractor in such manner as is necessary to reflect the position of the Subcontractor as a subcontractor to the Prime Contractor, to insure the Subcontractor's obligations to the Prime Contractor and to the U.S. Government, and to enable the Prime Contractor to meet its obligations under its Prime Contract. Clauses not requiring flow down from the Contractor to the Subcontractor, but nevertheless specified herein shall have full force and effect in performance of this Subcontract.

**Clauses Incorporated by Reference**
This Subcontract incorporates one or more of the following clauses by reference, suitably modified to properly identify the parties, with same force and effect as if they were given in full text. The complete text will be made available to Subcontractor upon request. The full text may also be accessed electronically at the following website: http://www.arnet.gov/far/

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

## SECTION H - SPECIAL CONTRACT REQUIREMENTS

### H.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 FAR clause.

### H.3 AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this contract is 935 for the prime contract.

## H.4 DEFENSE BASE ACT (DBA) INSURANCE

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

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

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

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

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

## H.5 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.

## H. 6 ELECTRONIC PAYMENTS SYSTEM

1. Definitions:
    a. "Cash Payment System" means a payment system that generates any transfer of funds through a transaction originated by cash, check, or similar paper instrument. This includes electronic payments to a financial institution or clearing house that subsequently issues cash, check, or similar paper instrument to the designated payee.

    b. "Electronic Payment System" means a payment system that generates any transfer of funds, other than a transaction originated by cash, check, or similar paper instrument, which is initiated through an electronic terminal, telephone, mobile phone, computer,

or magnetic tape, for the purpose of ordering, instructing or authorizing a financial institution to debit or credit an account. The term includes debit cards, wire transfers, transfers made at automatic teller machines, and point-of-sale terminals.

2. The contractor agrees to use an electronic payment system for any payments under this award to beneficiaries, subcontractors, or grants under contracts, where applicable.

3. Exceptions. The contractor is allowed the following exceptions, provided the contractor documents its contract file with the appropriate justification:

   a. Cash payments made while establishing electronic payment systems, provided that this exception is not used for more than six months from the effective date of this award.

   b. Cash payments made to payees where the contractor does not expect to make payments to the same payee on a regular, recurring basis, and payment through an electronic payment system is not reasonably available.

   c. Cash payments to vendors below the micro purchase level as defined by FAR 2.101, or for Grants Under Contracts for less than $3000, when payment through an electronic payment system is not reasonably available.

   d. The contractor has received a specific written exception from the Contracting Officer that a specific payment or all cash payments are authorized, based on the contractor's written justification, which provides a basis and cost analysis for the requested exception.

4. More information about how to establish, implement, and manage electronic payment methods is available to contractors at http://solutionscenter.nethope.org/programs/c2e-toolkit."

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

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

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

(2) "Intellectual Work" includes all works that document the implementation, monitoring, evaluation, and results of international development assistance activities developed or acquired under this award,

which may include program and communications materials, evaluations and assessments, information products, research and technical reports, progress and performance reports required under this award (excluding administrative financial information), and other reports, articles and papers prepared by the contractor under the award, whether published or not. The term does not include the contractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information.

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

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

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

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

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

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

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

**H.8 LANGUAGE AND MEASUREMENT (JUN 1992)**

(a) The English language shall be used in all written communications between the parties under this contract with respect to services to be rendered and with respect to all documents prepared by the contractor except as otherwise provided in the contract or as authorized by the contracting officer.

(b) Wherever measurements are required or authorized, they shall be made, computed, and recorded in metric system units of measurement, unless otherwise authorized by USAID in writing when it has found that such usage is impractical or is likely to cause U.S. firms to experience

significant inefficiencies or the loss of markets. Where the metric system is not the predominant standard for a particular application, measurements may be expressed in both the metric and the traditional equivalent units, provided the metric units are listed first.

## H.9 USAID DISABILITY POLICY (DEC 2004)

(a) The objectives of the USAID Disability Policy are:

(1) To enhance the attainment of United States foreign assistance program goals by promoting the participation and equalization of opportunities of individuals with disabilities in USAID policy, country and sector strategies, activity designs and implementation;

(2) To increase awareness of issues of people with disabilities both within USAID programs and in host countries;

(3) To engage other U.S. Government agencies, host country counterparts, governments, implementing organizations and other donors in fostering a climate of nondiscrimination against people with disabilities; and

(4) To support international advocacy for people with disabilities. The full text of USAID's policy can be found at the following Web site: *http://pdf.usaid.gov/pdf_docs/PDABQ631.pdf*.

(b) USAID therefore requires that the contractor not discriminate against people with disabilities in the implementation of USAID programs and that it 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.

## H.10 NONDISCRIMINATION (JUN 2012)

FAR part 22 and the clauses prescribed in that part prohibit contractors performing in or recruiting from the U.S. from engaging in certain discriminatory practices.

USAID is committed to achieving and maintaining a diverse and representative workforce and a workplace free of discrimination. Based on law, Executive Order, and Agency policy, USAID prohibits discrimination in its own workplace on the basis of race, color, religion, sex (including pregnancy and gender identity), national origin, disability, age, veteran's status, sexual orientation, genetic information, marital status, parental status, political affiliation, and any other conduct that does not adversely affect the performance of the employee. USAID does not tolerate any type of discrimination (in any form, including harassment) of any employee or applicant for employment on any of the above-described bases.

Contractors are required to comply with the nondiscrimination requirements of the FAR. In addition, the Agency strongly encourages all its contractors (at all tiers) to develop and enforce nondiscrimination policies consistent with USAID's approach to workplace nondiscrimination as described in this clause, subject to applicable law.

(End of clause)

## H.11 MEDICAL EVACUATION (MEDEVAC) SERVICES (JUL 2007)

(a) Contractor 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.

## H.12 USAID IMPLEMENTING PARTNER NOTICES (IPN) PORTAL FOR ACQUISITION (JUL 2014)

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

*"Universal" bilateral modification* means a bilateral modification, as defined in FAR subpart 43.1, that updates or incorporates new FAR or AIDAR clauses, other terms and conditions, or special requirements, affecting all USAID awards or a class of awards, as specified in the Agency notification of such modification.

*USAID Implementing Partner Notices (IPN) Portal for Acquisition (IPN Portal)* means the single point where USAID uploads universal bilateral modifications, which can be accessed electronically by registered USAID contractors. The IPN Portal is located at *https://sites.google.com/site/ipnforacquisitions/*.

*IPN Portal Administrator* means the USAID official designated by the M/OAA Director, who has overall responsibility for managing the USAID Implementing Partner Notices Portal for Acquisition.

(b) By submission of an offer and execution of a contract, the Offeror/Contractor acknowledges the requirement to:

(1) Register with the IPN Portal if awarded a contract resulting from this solicitation; and

(2) Receive universal bilateral modifications of this contract and general notices through the IPN Portal.

(c) *Procedure to register for notifications*. Go to: *https://sites.google.com/site/usaidipnforacquisitions/* and click the "Register" button at the top of the page. Contractor representatives must use their official organization email address when subscribing, not personal email addresses.

(d) *Processing of IPN portal modifications*.

(1) The contractor may access the IPN Portal at any time to review all IPN Portal modifications; however, the system will also notify the contractor by email when the USAID IPN Portal Administrator uploads a universal bilateral modification for contractor review and signature. Proposed IPN Portal modifications distributed through the IPN Portal are applicable to all awards, unless otherwise noted in the proposed modification.

(2) Within 15 calendar days from receipt of the notification email from the IPN Portal, the contractor must do one of the following:

(i)(A) Verify applicability of the proposed modification to their award(s) per the instructions provided with each modification;

(B) Download the modification and incorporate the following information on the SF30 form: contract number, organization name, and organization mailing address as it appears in the basic award;

(C) Sign the hardcopy version; and

(D) Send the signed modification (by email or hardcopy) to the contracting officer for signature;

*Note to paragraph (d)(2)(i)*: The contractor must not incorporate any other changes to the IPN Portal modification.

(ii) Notify the Contracting Officer in writing if the modification requires negotiation of the additional changes to terms and conditions of the contract; or

(iii) Notify the contracting officer that the contractor declines to sign the modification.

(3) Within 30 calendar days of receipt of a signed modification from the contractor, the contracting officer must provide the fully executed modification to the contractor or initiate discussions with the contractor. Bilateral modifications provided through the IPN Portal are not effective until both the contractor and the contracting officer sign the modification.

(End of clause)

**"H.13 CONTRACTOR ACCESS TO USAID FACILITIES AND USAID'S INFORMATION SYSTEMS (APRIL 2018) (DEVIATION NO. M/OAA-DEV-AIDAR-18-2c)**

(a) HSPD-12 and Personal Identity Verification (PIV). Individuals engaged in the performance of this award as employees, consultants, or volunteers of the contractor must

comply with all applicable Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV) procedures, as described below, and any subsequent USAID or Government- wide HSPD-12 and PIV procedures/policies.

(b) A U.S. citizen or resident alien engaged in the performance of this award as an employee, consultant, or volunteer of a U.S firm may obtain access to USAID facilities or logical access to USAID's information systems only when and to the extent necessary to carry out this award and in accordance with this clause. The contractor's employees, consultants, or volunteers who are not U.S. citizens or resident aliens as well as employees, consultants, or volunteers of non-U.S. firms, irrespective of their citizenship, will not be granted logical access to U.S. Government information technology systems (such as Phoenix, GLAAS, etc.) and must be escorted to use U.S. Government facilities (such as office space).

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

(2) Before a contractor (or a contractor employee, consultant, or volunteer) or subcontractor at any tier may obtain a USAID ID (new or replacement) authorizing the individual routine access to USAID facilities in the United States, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form to the Enrollment Office personnel when undergoing processing. One identity source document must be a valid Federal or State Government-issued picture ID. Contractors may contact the USAID Security Office to obtain the list of acceptable forms of documentation. Submission of these documents, to include documentation of security background investigations, is mandatory in order for the Contractor to receive a PIV/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18-2c, and M/OAA-DEV-AIDAR-18-2c) 10

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

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

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

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

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

(End of Clause)

## H.14 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.

(End of Clause)

## H.15 SOFTWARE LICENSE ADDENDUM (MAY 2016)

*(a)* This special contract requirement incorporates certain terms and conditions relating to Federal procurement actions. The terms and conditions of this Addendum take precedence over the terms and conditions contained in any license agreement or other contract documents entered into between the parties.

*(b)* Governing Law: Federal procurement law and regulations, including the Contract Disputes Act, 41 U.S.C. Section 601 et. seq., and the Federal Acquisition Regulation (FAR), govern the agreement between the parties. Litigation arising out of this contract may be filed only in those fora that have jurisdiction over Federal procurement matters.

*(c)* Attorney's Fees: Attorney's fees are payable by the Federal government in any action arising under this contract only pursuant to the Equal Access in Justice Act, 5 U.S.C. Section 504.

*(d)* No Indemnification: The Federal government will not be liable for any claim for indemnification; such payments may violate the Anti-Deficiency Act, 31 U.S.C. Section 1341(a).

*(e)* Assignment: Payments may only be assigned in accordance with the Assignment of Claims Act, 31 U.S.C. Section 3727, and FAR Subpart 32.8, "Assignment of Claims."

*(f)* Patent and Copyright Infringement: Patent or copyright infringement suits brought against the United States as a party may only be defended by the U.S. Department of Justice (28 U.S.C. Section 516).

*(g)* Renewal of Support after Expiration of this Award: Service will not automatically renew after expiration of the initial term of this agreement.

*(h)* Renewal may only occur in accord with (1) the mutual agreement of the parties; or (2) an option renewal clause allowing the Government to unilaterally exercise one or more options to extend the term of the agreement.

(End of Clause)

## H.16 ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY (APRIL 2018)

*(a) Definitions*

"Information and Communication Technology (ICT) means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; Web sites; videos; and, electronic documents. (Appendix A to Part 1194 – Section 508 of the Rehabilitation Act)

*(b)* Federal agencies are required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to information and communication technology for disabled individuals within its employment, and for disabled members of the public seeking information and services. This access must be comparable to that which is offered to similar individuals who do not have disabilities. Standards for complying with this law are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board"). The contractor must comply with any future updates of standards by the Access Board. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.access-board.gov/sec508/508standards.htm.

*(c)* Except as indicated elsewhere in the contract, all ICT procured through this contract must meet the applicable accessibility standards at 36 CFR 1194 as follows:

1194.21 Software applications and operating systems
1194.22 Web-based intranet and Internet information and applications
1194.23 Telecommunications products 1194.24 Video and multimedia products 1194.25 Self-contained, closed products
1194.26 Desktop and portable computers 1194.31 Functional performance criteria
1194.41 Information, documentation, and support

*(d)* Deliverable(s) must incorporate these standards as well.

*(e)* The final work product must include documentation that the deliverable conforms with the Section 508 Standards promulgated by the US Access Board.

*(f)* The Contractor must comply with 508 standards, and any changes needed to conform to the standards will be at no additional charge to USAID.

(End of Clause)

**H.17 INFORMATION TECHNOLOGY APPROVAL (APRIL 2018) (DEVIATION NO. M/OAA- DEV-FAR-18-2C)**

(1) Definitions. As used in this contract – "Information Technology" means Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

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

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

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

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

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

(d) Request for Approval Requirements:

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

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

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

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

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

(End of Clause)

**H.18 MEDIA AND INFORMATION HANDLING AND PROTECTION (APRIL 2018)**

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

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. This also includes but not limited to all records, files, and metadata in electronic or hardcopy format.

"Sensitive Information or Sensitive But Unclassified" (SBU) means information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05- 26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers "Media" means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

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

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

1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.
2) Proper security, control, and storage of mobile technology, portable data storage devices, and communication devices.
3) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information while at rest and in transit throughout USAID, contractor, and/or subcontractor networks, and on host and client platforms.
4) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

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

(e) Destruction of Sensitive Information: Within twenty (20) business days after USAID has received

all Agency records and media, the Contractor must execute secure destruction (either by the contractor or third party firm approved in advance by USAID) of all remaining originals and/or copies of information or media provided by USAID and/or obtained by the Contractor while conducting activities in accordance with the contract. After the destruction of all information and media, the contractor must provide USAID with written confirmation verifying secure destruction.

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

(End of Clause)

**H.19 PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEMS INCIDENT REPORTING (APRIL 2018)**

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

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

"Sensitive Information" or "Sensitive But Unclassified" Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers,

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

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

"Information Security Incident" means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an

information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. “Spillage” means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited,(i.e., authorized) for the applicable security level of the data or information.

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

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

(c) Privacy Act Compliance

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

(d) IT Security and Privacy Training

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

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

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

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

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

(e) Information Security and Privacy Incidents

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

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

Contractor Facilities Security Officer.

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

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

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

(2) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information (PII), and can result in the loss of the public's trust and confidence in the Agency's ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Contractor employees must report (by e-mail) all Privacy Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the incident, at: CIO- HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer's representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read "Action Required: Potential Privacy Incident".

(3) Information Security Incident Response Requirements

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

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

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

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

v. All determinations related to an Information Security Incident associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract will be made only by the USAID CIO through the CO or COR.
vi. The Contractor must report criminal activity to law enforcement organizations upon becoming aware of such activity.

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

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

(End of Clause)

**H.20 SKILLS AND CERTIFICATION REQUIREMENTS FOR PRIVACY AND SECURITY STAFF (APRIL 2018)**

(a) Applicability: This special contract requirements applies to the Contractor, its subcontractors and personnel providing support under this contract and addresses the Privacy Act of 1974 (5 U.S.C. 552a - the Act), the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347, 44 U.S.C. 3531-3536), and Federal Information Security Modernization Act (FISMA) of 2014 (FISMA, Public Law 113-283 44 U.S.C. 3531-3536, as amended).

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

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

(End of Clause)

**H.21 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APRIL 2018)**

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

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

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

Nation.

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

"Sensitive" Information or Sensitive But Unclassified (SBU) - Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers.

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

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

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

(c) Compliance with IT Security and Privacy Policies: The contractor shall be responsible for implementing information security for all information systems procured, developed, deployed, and/or operated on behalf of the US Government. All Contractor personnel performing under this contract and Contractor equipment used to process or store USAID data, or to connect to USAID networks, must comply with Agency information security requirements as well as current Federal regulations and guidance foundin 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.

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

5 Security Monitoring, Auditing and Alerting Requirements: All Contractor-owned and operated systems that use or store USAID information must meet or exceed standards documented in this contract and in Service Level Agreements and Memorandums of Understanding/Agreements pertaining to security monitoring and alerting. These requirements include but are not limited to: Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18-2c, and M/OAA-DEV-AIDAR-18- 2c) 29 System and Network Visibility and Policy Enforcement at the following levels:

- Edge
- Server / Host
- Workstation / Laptop / Client
- Network
- Application
- Database
- Storage
- User

- Alerting and Monitoring
- System, User, and Data Segmentation

6. Contractor System Oversight/Compliance
    - 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.
7. Security Assessment and Authorization (SA&A)
    - 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.
    - 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.
    - 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.
    - 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.
    - All documentation must be prepared, stored, and managed in accordance with standards,

templates and guidelines established by USAID M/CIO. The USAIDM/CIO or designee must approve all SA&A requirements.

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

a. 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.

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

(End of Clause)

**H.22 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 or 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 inthe provisions of this contract and National Archives and Records Administration (NARA) retention policies.

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

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

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

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

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

(g) Information Security Incidents

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

i. Contractor employees must report via e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming

aware of the Incident, at: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the Contracting Officer and Contracting Officer's representative and the Contractor Facilities Security Officer. Contractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Contractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

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

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

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

(j) Security Requirements:

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

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

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

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

(5) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report must be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18- 2c, and M/OAA-DEV-AIDAR-18-2c) 37 Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.

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

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

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

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

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

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have been resolved or mitigated. Additionally, at USAID’s request, the Contractor must submit reports or provide a dashboard where USAID can continuously verify that service levels are being met. Where SLAs fail to be met, USAID may assess monetary penalties or service credit.

(o) Trusted Internet Connection (TIC): The Contractor must route all USAID traffic through the TIC. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT)

(p) Forensics, Freedom of Information Act (FOIA), Electronic Discovery, or additional Information Requests: The Contractor must allow USAID access required to retrieve information necessary for FOIA and Electronic Discovery activities, as well as, forensic investigations for both criminal and noncriminal purposes without their interference in these activities. USAID may negotiate roles and responsibilities for conducting these activities in agreements outside of this contract.
   (1) The Contractor must ensure appropriate forensic tools can reach all devices based on an approved timetable.
   (2) The Contractor must not install forensic software or tools without the permission of USAID.
   (3) The Contractor, in coordination with USAID Bureau for Management, Office of The Chief Information Officer (M/CIO)/ Information Assurance Division (IA), must document and preserve data required for these activities in accordance with the terms and conditions of the contract.
   (4) The Contractor, in coordination with USAID M/CIO/IA, must clearly define capabilities, procedures, roles and responsibilities and tools and methodologies for these activities.

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

(End of Clause)

## H.27 ADS 302.3.5.19 USAID-FINANCED THIRD-PARTY WEB SITES (AUG 2013)

(a) Definitions:

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

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

(1) Working through the COR, the contractor must notify the USAID Bureau for Legislative and Public Affairs/Public Information, Production and Online Services (LPA/PIPOS) of the Web site URL as far in advance of the site's launch as possible.

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

(3) The Web site must be marked on the index page of the site and every major entry point to the Web site with a disclaimer that states:

"The information provided on this Web site is not official U.S. Government information and does not represent the views or positions of the U.S. Agency for International Development or the U.S. Government."

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

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

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

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

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

## H.28 FOREIGN GOVERNMENT DELEGATIONS TO INTERNATIONAL CONFERENCES (AUGUST 2016)

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 [http://www.usaid.gov/policy/ads/300/350maa.pdf] or as approved by the CO.

## H.29 ADS 302.3.5.20 CONFERENCE PLANNING AND REQUIRED APPROVALS (AUGUST 2013)

The contractor must obtain USAID approval prior to committing costs related to conferences funded in whole or in part with USAID funds where:

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

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

A conference is defined as a seminar, meeting, retreat, symposium, workshop, training activity or other such event that requires temporary duty travel of USAID employees. For the purpose of this policy, an

employee is defined as a U.S. direct hire; personal services contractor, including U.S. PSCs, Foreign Service National (FSN)/Cooperating Country National (CCN) and Third Country National (TCN); or a Federal employee detailed to USAID from another government agency. Conferences approved at the time of award will be incorporated into the award. Any subsequent requests for approval of conferences must be submitted by the contractor to the USAID COR. The COR will obtain the required agency approvals and communicate such approvals to the contractor in writing. The request for conference approval must include:

- A brief summary of the proposed event;
- A justification for the conference and alternatives considered, e.g., teleconferencing and videoconferencing;
- The estimated budget by line item (e.g., travel and per diem, venue, facilitators, meals, equipment, printing, access fees, ground transportation);
- A list of USAID employees attending and a justification for each; and the number of other USAID-funded participants (e.g., institutional contractors);
- The venues considered (including government-owned facility), cost comparison, and justification for venue selected if it is not the lowest cost option;
- If meals will be provided to local employees (a local employee would not be in travel status), a determination that the meals are a necessary expense for achieving Agency objectives; and
- A certification that strict fiscal responsibility has been exercised in making decisions regarding conference expenditures, the proposed costs are comprehensive and represent the greatest cost advantage to the U.S. Government, and that the proposed conference representation has been limited to the minimum number of attendees necessary to support the Agency's mission.

**[END OF SECTION H]**

**[END OF ATTACHMENT D]**