Acquisition & Assistance Policy Directive (AAPD)

From the Director, Office of Acquisition & Assistance Issued: May 3, 2016

AAPD 16-02

SPECIAL CONTRACT REQUIREMENTS FOR INFORMATION TECHNOLOGY (IT) (Class Deviations M/OAA-DEV-FAR-16-1c and M/OAA-DEV-AIDAR-16-2c)

Subject Category: Acquisition Management
Type: POLICY

AAPDs provide information of significance to all agency personnel and partners involved in the Acquisition and Assistance process. Information includes (but is not limited to): advance notification of changes in acquisition or assistance regulations; reminders; procedures; and general information. Also, AAPDs may be used to implement new requirements on short-notice, pending formal amendment of acquisition or assistance regulations.

AAPDs are EFFECTIVE AS OF THE ISSUED DATE unless otherwise noted in the guidance below; the directives remain in effect until this office issues a notice of cancellation.

This AAPD: ☒ Is New ☐ Replaces/ ☐ Amends CIB/AAPD

Applicable to: ☒ Existing awards; ☒ Modification required ☐ No later than ☒ As noted in guidance below ☒ RFPs issued on or after the effective date of this AAPD; all other Pending Awards, i.e., 8(a), sole source, IQC ☐ Other	Precedes change to: ☒ AIDAR Part(s) 752 and 704 Appendix ☐ USAID Automated Directives System (ADS) Chapter ☐ Code of Federal Regulations ☐ Federal Acquisition Regulations ☐ No change to regulations

☒ New Provision/Clause/Special Contract Requirement Provided Herein: GLAAS Update - 30 days after the effective date

/s/
Roy Plucknett

1. **Purpose:**

The purpose of this AAPD is to provide new special contract requirements and revised AIDAR clause 752.204-72 Access to USAID Facilities and USAID's Information Systems to ensure compliance with federal Information Technology (IT) security and accessibility requirements and guidelines, such as Federal Information Security Management Act (FISMA), OMB Circular A-130 Management of Federal Information Resources, M-14-03 Enhancing the Security of Federal Information and Information Systems, and others as specified in the revised clause/special contract requirements.

Required Action:
Contracting Officers (COs) must insert the attached revised clause/special contract requirements in solicitations and resulting awards (irrespective of award value) in accordance with the guidance below.
Note that this applies to solicitations and resulting contracts for supplies and/or services that include an IT supplies/services component (including cloud services), or include a requirement that the contractor have access to sensitive information. Per the revised definition of IT below, the special contract requirements are applicable to any equipment/services or system(s) used by the Agency directly or used by a contractor under a contract that requires use of the services or equipment or system(s). IT procured for host countries, e.g., Health Information System for Government of Kenya, laptops for El Salvador public schools, etc., is not subject to these special requirements.

2. **Background:**

The increasing dependency on Information Technology (IT) systems and networked operations pervades nearly every aspect of the world and global economies. While bringing significant benefits, this dependency also introduces vulnerabilities to cyber-based threats. As such, cybersecurity is one of the most serious economic and national security challenges we face. This underscores the importance of safeguarding critical and sensitive information and information systems.

The increasing number and severity of data breaches and cyber security incidents have resulted in real costs and consequences to the Federal government and global partners around the world. This becomes more significant as Federal Agencies, including USAID, increasingly rely on contractors for a variety of information technology (IT) services. The federal government recognizes the seriousness of cybersecurity and is committed to improving safeguards for information and information systems that support the operations and assets of federal agencies, including those provided or managed by other federal entities and contractors. The Office of Management and Budget's (OMB) analysis of an increasing number of cybersecurity events, both within and outside of government, indicates that a majority of these incidents are preventable through implementation of basic cybersecurity practices and procedures. In order to manage risks and threats effectively, agency leadership must continue to focus on improving cybersecurity, and ensure the implementation of these basic cybersecurity procedures.

The Office of Management and Budget (OMB) and the National Security Council (NSC) convened a President's Management Council, with one of the focus areas being improvement of cybersecurity in Federal acquisitions, in particular, accountability of contractors providing IT systems and services to the Federal government. On September 5, 2014, the President's Management Council required agencies to review IT contracts, identify gaps in cybersecurity contracts and contract language, and provide OMB and the NSC a summary of findings and actions taken to mitigate identified gaps. In response, USAID drafted a memo "Memorandum for the OMB Deputy Director for Management and the NSC Assistant to the President for Homeland Security and Counterterrorism," dated October 31, 2014, certifying that the Agency had completed the required cybersecurity assessments and detailed its findings and actions taken. One of the actions USAID detailed in the memo was that it will establish and implement a process to identify and review contracts to ensure compliance with Federal IT security requirements and guidelines to include FISMA, OMB Circular A-130, M-14-03, M-14-04[1], and National Institute of Standards and Technology (NIST) Standards SP 800-137[2].

As part of this effort, the Bureau For Management, Office of the Chief Information Officer (M/CIO), coordinated with the Office of Acquisition and Assistance (M/OAA) and the Office of General Counsel (OGC) to develop special requirements for contracts to ensure that the Agency's information systems and contractors supporting such systems can meet the Federal security guidelines specified by OMB. Two class deviations were approved by the M/OAA Director: 1) Class Deviation # M/OAA-DEV-FAR-16-1c which revised the FAR 2.101(b) Definition of Information Technology, and 2) Class Deviation # M/OAA-DEV-AIDAR-16-2c which revised AIDAR Clause 752.204-72, Contractor Access to USAID Facilities and Information Technology Systems, to incorporate updated procedures in managing Contractor access. The IT special contract requirements will assist requiring bureaus, offices and missions ensure that appropriate privacy, cybersecurity, or other requirements are met in their awards.

M/CIO and M/OAA will initiate formal rule-making procedures immediately to incorporate the revised clause along with the new special contract requirements into the AIDAR.

3. **Guidance:**

a. The Director, M/OAA has approved the following two class deviations:

1) Class Deviation #M/OAA-DEV-FAR-16-1c, FAR 2.101 Definitions.

The definition of "information technology" as currently defined in FAR 2.101 is revised to read as follows:

"(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation,

[1] "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

[2] Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

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."

The current FAR definition of IT is not broad enough to include cloud computing services; the approved expanded definition is provided in the applicable special requirements in Attachment 1. It aligns with OMB guidance that was promulgated in support of the Federal Information Technology Acquisition Reform Act (FITARA) and related IT management practices in OMB Memo M-15-14, titled Management Oversight of Federal Information Technology". It is anticipated that the FAR Council will take measures to officially and similarly revise the definition of IT during 2016 in order to establish a consistent government-wide definition.

2) Class Deviation # M/OAA-DEV-AIDAR-16-2c to AIDAR 752.204-72 Access to USAID Facilities and USAID's Information Systems

This clause is required for those contracts that require the contractor, contractor employee, or consultant (and/or subcontractor, subcontractor employee, or consultant) to have routine physical access to USAID space or logical access to USAID's information systems. This clause has been revised to add specific timeframes for the contractor to submit requests for access and termination of access, as well as monthly staffing reports to enable better oversight of contractor personnel access.

b. Effective immediately, COs must insert the applicable special contract requirements/ revised clause into solicitations and resulting contracts for: 1) IT supplies and/or services and 2) supplies and/or services that include an IT supplies and/or services component, or a requirement that the contractor have access to sensitive information.

The applicable special contract requirements and the revised clause are provided in Attachment 1 - Revised Clause AIDAR 752.204-72 Access to USAID Facilities and

USAID's Information Systems and Attachment 2 - Special Contract Requirements for Information Technology. COs must also insert the Special Contract Requirements for Information Technology and the AIDAR Clause 752.204-72 into existing high-risk contracts as determined by M/OAA and M/CIO. COs must insert, as applicable, the Special Contract Requirements for Information Technology into Section H – Special Contract Requirements of the solicitation/award. The attachments provide agency-specific requirements to supplement applicable FAR, AIDAR, and ADS 302 guidance, such as 52.204-9, Personal Identity Verification of Contractor Personnel, 52.204-2 Security Requirements, and 52.224–2 Privacy Act (when the design, development, or operation of a system of records on individuals is required to accomplish an agency function).

COs must work with Contracting Officer Representatives (CORs) to identify affected solicitations and resulting awards. In addition, COs should ensure that CORs are made aware of the new/revised requirements as there are additional responsibilities for contract deliverables and approvals.

4. Points Of Contact:

USAID Contracting Officers may direct their questions about this AAPD to Carol Ketrick at cketrick.usaid.gov or telephone: 202-567-4676. For questions specific to IT regulations and policies, contact: Bruce Wierzechowski at e-mail: bwierzechowski@usaid.gov or telephone 703-666-542; for questions on implementation of Section 508 only, contact: William Morgan at e-mail: wmorgan@usaid.gov, telephone: 703-666-5691.

Attachments:

1 - Revised Clause AIDAR 752.204-72 Access to USAID Facilities and USAID's Information Systems
2 - Special Contract Requirements for Information Technology

Attachment 1 -
Revised Clause AIDAR 752.204-72 Access to USAID Facilities and USAID's Information Systems

Insert 752.204-72, Contractor Access to USAID Facilities and Information Technology Systems, in solicitations and contracts when FAR 52.204-9, Personal Identity Verification of Contractor Personnel, is used.

1. AIDAR 752.204-72 Access to USAID Facilities and USAID's Information Systems.

As prescribed in (48 CFR) AIDAR 704.404(b), insert the following clause in all solicitations and contracts that contain the provision at (48 CFR) FAR 52.204-9:

752.204-72 Access to USAID Facilities and USAID's Information Systems (MAY 2016)

(DEVIATION NO. M/OAA-DEV-AIDAR-16-2c)

(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 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, are mandatory in order for the contractor to receive a PIV/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment.

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

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

(f) USAID, at its discretion, may suspend or terminate the access to any systems and/or facilities when an 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 (CIO-HELPDESK@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)

Attachment 2 - Special Contract Requirements for Information Technology

1. Restrictions Against Disclosure

Insert the following special contract requirement in services contracts, including information technology and architect-engineer contracts, supply contracts, and construction contracts requiring a restriction on the release of information developed or obtained in connection with performance of the contract.

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)

2. Software License

Insert the following special contract requirement in solicitations and contracts for new software licenses or to renew existing licenses.

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)

3. **Electronic and Information Technology Accessibility**

Insert the following special contract requirement in solicitations and contracts which include acquisition of Electronic and Information Technology (EIT) supplies and/or services.

Electronic and Information Technology Accessibility (MAY 2016)

(a) Federal agencies are required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to electronic and information 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.

(b) Except as indicated elsewhere in the contract, all electronic and information technology (EIT) 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

(c) Deliverable(s) must incorporate these standards as well.

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

(e) 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)

4. Use of Information Technology Notification

Insert the following special contract requirement in all USAID solicitations and contracts for Information Technology (IT) or include a component for IT as defined within this special requirement. This requirement applies when the IT services/supplies are for use by the Agency directly or by a contractor under a contract that requires use of the services or equipment or system(s). This requirement is not applicable for any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment

Use of Information Technology Notification (MAY 2016) (DEVIATION NO. M/OAA-DEV-FAR-16-1c)

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

“Information Technology” means

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

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

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

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

(b) 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), 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), Federal Information Security Management Act (FISMA) of 2002, Federal Information Technology Acquisition Reform Act (FITARA) and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data. The following should not be construed to alter or diminish civil and/or criminal liabilities provided under various laws or mandates.

(c) Notification Requirements: 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.

(1) The Contracting Officer’s written confirmation of the Agency CIO approval must be in place prior to starting work on the information technology component(s) of the contract. If approval has not already been obtained, the Contractor must work through the Contracting Officer and Contracting Officer Representative (COR) to do so immediately. Please refer to paragraph (3) below for notification procedures.

(2) The Contractor shall notify the Contracting Officer in writing whenever it becomes aware that any IT equipment, software or services necessary to meet the Government’s requirement or to facilitate

activities in the Government's statement of work were not disclosed in the schedule or statement of work.

(3) As part of the notification, the Contractor shall provide the Contracting Officer an estimate of the total cost of the IT equipment, software, and associated services regarding this contract and to obtain approval for procurement, development or modifications. The Contractor must simultaneously notify COR and the Office of the Chief Information Office at ITAuthorization@usaid.gov.

(4) Except as required by other provisions of this contract, specifically stated to be an exception to this special contract requirement, the Government is not obligated to reimburse the Contractor for costs incurred in excess of the IT equipment, software or services specified in the Schedule.

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

(End)

5. Media and Information Handling and Protection

Insert the following special contract requirement in all USAID solicitations and contracts for Information Technology services for where contractors may be required to handle Sensitive Information as defined in the special contract requirement. This requirement applies when the IT services are for use by the Agency directly or by a contractor under a contract that requires use of the services or equipment or system(s). This requirement is not applicable for any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment (see definition of IT in special requirement "**Use of Information Technology Notification (MAY 2016)"**.

Media and Information Handling and Protection (MAY 2016)

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

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

"Sensitive Information or Sensitive But Unclassified" (SBU) means information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a

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

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

(c) Handling and Protection. The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Within 45 calendar days of the award, the Contractor must develop policies or documentation regarding the protection, handling, and destruction of Sensitive Information The policy or procedure must address at a minimum, the requirements documented in NIST 800-53 Revision 4 or the current revision for Media Protection Controls as well as the following:

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

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

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

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

(d) Return of all USAID Agency records.

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

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

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

(End)

6. Privacy and Security Requirements

Insert the following special contract requirement in all solicitations and contracts for the design, development, or operation of a System of Records on individuals to accomplish an agency function and 52.224-1, Privacy Act Notification and FAR 52.224–2 Privacy Act are used.

Privacy and Security Information Technology Systems Incident Reporting (MAY 2016)

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

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

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

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

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

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

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

(c) Privacy Act Compliance

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

(d) IT Security and Privacy Training

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

(2) The USAID Rules of Behavior must be signed by each user prior to gaining access to USAID information systems, periodically at the request of USAID, or whenever the Rules are updated. USAID will provide access to the rules of behavior and provide notification as required.

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

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

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

(e) Information Security and Privacy Incidents

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

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

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

(2) Privacy Incident Reporting Requirements: USAID must manage in accordance with Federal laws and regulations the information it collects, uses, maintains, and disseminates in support of its mission and business functions. Any unauthorized use, disclosure, or loss of such information can result

in the loss of the public's trust and confidence in the Agency's ability to protect it properly. PII breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. Therefore, incidents involving a breach of PII have a critical time-period for reporting. Contractor and Contractor staff must report immediately upon discovery all potential and actual privacy breaches to the Contracting Officer, the USAID Service Desk at 202-712-1234 or CIO-HELPDESK@usaid.gov, and the Privacy Office at privacy@usaid.gov, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred. The subject line shall read "Action Required: Potential Privacy Incident".

(3) Incident Response Requirements

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

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

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

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

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

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

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

In altering this special contract requirement, require subcontractors to report information security and privacy incidents directly to at the USAID Service Desk at 202-712-1234 or CIO-HELPDESK@usaid.gov/ and the Privacy Office at privacy@usaid.gov. A copy of the correspondence

shall be sent to the prime Contractor (or higher tier subcontractor) and the Contracting Officer referencing the ticket number.

(End)

7. Skills and Certification Requirements for Privacy and Security Staff

Insert the following special contract requirement in solicitations and contracts for Information Technology (IT) services or include a component for IT services. This requirement applies when the IT services are for use by the Agency directly or by a contractor under a contract that requires use of the services or equipment or system(s). This requirement is not applicable for any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment (see definition of IT in special requirement "**Use of Information Technology Notification (MAY 2016)"**.

Skills and Certification Requirements for Privacy and Security Staff (MAY 2016)

(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) and Federal Information Security Management Act (FISMA) of 2002 (FISMA, Public Law 107-347. 44 U.S.C. 3531-3536).

(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)

8. Security Requirements for Unclassified Information Technology Resources

Insert Security Requirements for Unclassified Information Technology Resources in all USAID solicitations and contracts for Information Technology (IT) services or include a component for IT

services. This requirement applies when the IT services are for use by the Agency directly or by a contractor under a contract that requires use of the services or equipment or system(s). This requirement is not applicable for any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment (see definition of IT in special requirement "**Use of Information Technology Notification (MAY 2016)"**.

Security Requirements for Unclassified Information Technology Resources (MAY 2016)

(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 information technology resources include, but are not limited to, IT services, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(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 sufficient Information Technology security, to reasonably prevent the compromise of USAID IT resources for all of the Contractor's systems that are interconnected with a USAID network or USAID systems that are operated by the contractor. All Contractor personnel performing under this contract and Contractor equipment used to process or store USAID data, or to connect to USAID networks, must comply with Agency IT cybersecurity requirements as well as current Federal regulations and guidance found in the Federal Information Security Management Act (FISMA), Privacy Act of 1974, E-Government Act of 2002, Section 208, National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other relevant Federal laws and regulations that are applicable to USAID. The Contractor must comply with the following:

(1) HSPD-12 Compliance

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

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

(2) Internet Protocol Version 6 (IPv6) or current version: This acquisition requires all functionality, capabilities and features to be supported and operational in both a dual-stack IPv4/IPv6 environment and an IPv6 only environment. Furthermore, all management, user interfaces, configuration options, reports and other administrative capabilities that support IPv4 functionality will support comparable IPv6

functionality. The Contractor is required to certify that its products have been tested to meet the requirements for both a dual-stack IPv4/IPv6 and IPv6-only environment. USAID reserves the right to require the Contractor's products to be tested within a USAID or third party test facility to show compliance with this requirement.

(3) Secure Configurations

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

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

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

iv. The Contractor must apply due diligence at all times to ensure that the required level of security is always in place to protect USAID systems and information, such as using Defense Information Systems Agency Security Technical Implementation Guides (STIGs), common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov 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. Encryption is required to protect federal and Contractor data at rest in some cases and when transmitting data between systems.

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

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

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

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

(6) Contractor System Oversight/Compliance

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

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

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

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

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

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

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

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

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

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

vi. In cases where the IT System is not the property of the government but processes Agency information, 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 at http://www.fedramp.gov/marketplace/accredited-3paos/. The Contractor must submit a signed SA&A package approved by the 3PAO to USAID at saacapackages@usaid.gov at least 60 days prior to obtain the ATO for the IT system.

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

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

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

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

(8) Federal Reporting Requirements: Contractors operating information systems on behalf of USAID must comply with FISMA reporting requirements. Monthly, quarterly and annual data collections will

be coordinated by USAID. Data collections include but are not limited to, data feeds in a format consistent with Office of Management and Budget (OMB) requirements. The Contractor must provide timely responses as requested by USAID and OMB.

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

(End)

9. Cloud Computing

Insert the following special contract requirement in all USAID solicitations and contracts for, or that include, the use of programs, storage and access of data hosted on a third party's IT network.

Cloud Computing (MAY 2016)

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

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

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

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

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

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

Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

"Penetration Testing" means security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

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

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

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

(b) **Computing**

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

(c) Limitations on access to, use and disclosure of, government data and Government-related data.

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

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

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

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

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

(d) Records Management and Access to Information

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

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

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

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

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

(f) Spillage and Security Incidents: Upon written notification by the Government of a spillage or security incident, or the Contractor's discovery of a spillage or security incident, the Contractor shall coordinate immediately with the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or security incident in compliance with agency-specific instructions.

(g) Information Ownership and Rights: USAID information stored in a cloud environment remains the property of USAID, not the Contractor or cloud service provider (CSP). USAID retains ownership of the information and any media type that stores Government information. The CSP does not have rights to the USAID information for any purposes other than those explicitly stated in the contract.

(h) Security Requirements:

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

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

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

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

(6) The Contractor is responsible for mitigating all security risks found during SA&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within thirty (30) days and all moderate risk vulnerabilities must be mitigated within sixty (60) days from the date vulnerabilities are formally identified. 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.

(i) 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.

(j) 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.

(k) PII Breach Response: The Contractor is responsible for timely breach reporting, individual notification, mitigation, cost and containment resulting from PII Breaches. The Contractor must document and provide to the COR and USAID Chief Privacy Officer (privacy@usaid.gov) a plan describing in detail their breach response policies and processes addressing these issues to include credit monitoring or other appropriate relief to affected individuals.

(l) 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.

(m) 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.

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

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

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

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

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

(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.

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

(End)