# PART 352—SOLICITATION PROVISIONS AND CONTRACT CLAUSES (DEVIATION)

## 352.204-72 RECORDS MANAGEMENT (FEB 2024) (DEVIATION)

(a) *Applicability*. This clause applies to contracts that include Federal records, as defined in paragraph (b).

(b) *Definition.* As used in this clause—

*Federal record* means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. See 44 U.S.C. 3301.

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by Contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with deliverables.

(2) *Recorded information* means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)

(3) *Personal materials* means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)

(c) *Requirements.*

(1) The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at 36 CFR chapter XII subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all Federal records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

(3) In accordance with 36 CFR 1222.32, the Contractor shall maintain all Federal records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

(5) The Contractor shall immediately notify the Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that appropriate personnel are trained to adhere to these contract requirements, and that applicable, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information, data, documentary material, Federal records and/or equipment is properly protected. The Contractor shall not remove Federal Records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, Federal records and/or equipment are no longer required, it shall be returned to HHS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or as otherwise directed by the Contracting Officer. Destruction of Federal records is expressly prohibited unless in accordance with paragraph (c)(4).

(6) The Contractor shall only use Government information technology equipment for purposes specifically authorized by the contract and in accordance with HHS policy.

(7) The Contractor shall not create or maintain any Federal records containing any non-public HHS information that are not specifically authorized by the contract.

(8) The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

(9) All Contractor employees assigned to this contract handle Federal records are required to take HHS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

(d) *Subcontract flowdown.* The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract.

(End of clause)

## 352.204-73 CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS (FEB 2024) (DEVIATION)

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

*Agency access* means access to HHS facilities, sensitive information, information systems or other HHS resources.

*Applicant* means a contractor employee for whom the Contractor applies for an HHS identification card.

*Contractor employee* means a prime contractor and subcontractor employee who requires agency access to perform work under an HHS contract.

*Identification card (or "ID card")* means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by HHS, or a non-PIV card issued by another Federal agency and approved by HHS. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.

*Issuing office* means the HHS entity that issues identification cards to contractor employees.

*Local security servicing organization* means the HHS entity that provides security services to the HHS organization sponsoring the contract.

(b) *Risk and sensitivity level designations*. For contracts requiring access to HHS facilities, sensitive information, information systems or other HHS resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. HHS will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. **The position sensitivity designation levels that apply will be identified in the contract.** The following risk and sensitivity level designations and associated level of processing are required, and each level includes the prior levels—

(1) Low risk level: National Agency Check with Written Inquiries (NACI);

(2) Moderate risk level: Minimum Background Investigation (MBI); and

(3) High risk level: Background Investigation.

(c) *Security clearances.* Contractor employees may also be required to obtain security clearances (*i.e.*, Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in HHS will be processed according to the HHS Personnel Security and Suitability Program, HHS Instruction 731-1, and the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

(d) *Pre-screening of contractor employees*. The Contractor must pre-screen individuals designated for employment under any HHS contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to HHS for agency access. HHS may decline to grant agency access to a contractor employee for reasons including, but not limited to—

(1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;

(2) Falsification of information entered on forms or of other documents submitted;

(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and

(4) Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

(e) *Citizenship status*. The Contractor must monitor a non-citizen’s continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

(f) *Background investigation and adjudication*. A contractor employee must have a favorable adjudication of background investigation before HHS will issue an ID card to the contractor employee granting access to HHS facilities, sensitive information, information systems or other HHS resources. HHS may accept favorable adjudications of background

investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. HHS may also accept PIV-I (Interoperable) cards issued by an authorized PIV-1 issuer as evidence of identity. A favorable adjudication does not preclude HHS from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before an HHS identification card can be issued. Each Contractor must use the Office of Personnel Management's (OPM) e-QIP system, or successor system identified by HHS, to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COR or Contracting Officer. The HHS Assistant Secretary for Administration, Program Support Center (PSC), or authorized HHS designee, is responsible for adjudicating the suitability of contractor employees.

(g) *Agency access denied*. Upon contract award, HHS will initiate the agency access procedure for all contractor employees requiring access to HHS facilities, sensitive information, controlled unclassified information, information systems, and other HHS resources for contract performance. HHS may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The Contractor must not provide agency access to contractor employees until the COR or Contracting Officer provides notice of approval, which is authorized only by the PSC, or authorized HHS designee. Where a proposed contractor employee is denied agency access by the Government or, if for any reason a proposed application is withdrawn by the Contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective pre-screening or planning on the part of the Contractor may be considered as part of the Contractor's overall performance evaluation.

(h) *Identification card application process*. The COR will be the HHS ID card Sponsor and point of contact for the Contractor's application for an HHS ID card. The COR shall review and approve the HHS ID card application before an ID card is issued to the applicant. An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COR may request the issuing office to waive the six-month eligibility requirement when it is in HHS interest for contract performance. The following applies—

(1) PIV card. The applicant must complete an HHS on-line application for a PIV card;

(2) Non-PIV card. The applicant must complete and submit a hard copy of the necessary form(s) to be provided to Contractor by COR/Sponsor) to the COR/Sponsor; and

(3) Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in person to provide two forms of identity source documents in original form to HHS. The identity source documents must come from the list of acceptable documents included in Form F-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document

must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

(i) *Identification card custody and control*. The Contractor is responsible for the custody and control of all forms of government identification issued by HHS to contractor employees for access to HHS facilities, sensitive information, information systems and other HHS resources. The Contractor shall:

(1) Provide a listing of personnel for whom an identification (ID) card is requested to the COR who will provide a copy of the listing to the card issuing office. This may include Contractor and subcontractor personnel. Follow issuing office directions for submittal of an application package(s).

(2) While visiting or performing work on an HHS facility, as specified by the issuing office or COR, ensure that contractor employees prominently display their ID card.

(3) Immediately notify the COR or, if the COR is unavailable, the Contracting Officer when a contractor employee's status changes and no longer requires agency access (*e.g.*, employee's transfer, completion of a project, retirement, removal from work on the contract, or termination of employment) that may affect the employee's eligibility for access to the facility, sensitive information, or resources.

(4) Promptly deliver to the issuing office: (a) all ID cards assigned to an employee who no longer requires access to the facility; and (b) all expired ID cards within five (5) days of their expiration or all cards at time of contract termination, whichever occurs first.

(5) Immediately report any lost or stolen ID cards to the issuing office and follow its instructions.

(i) The Contractor is responsible for maintaining and safeguarding the HHS ID card upon issuance to the contractor employee. The Contractor must ensure that contractor employees comply with HHS requirements concerning the renewal, loss, theft, or damage of an ID card. The Contractor must immediately notify the COR or, if the COR is unavailable, the Contracting Officer when an ID card is lost, stolen or damaged.

(ii) Failure to comply with the requirements for custody and control of HHS ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to HHS facilities, sensitive information, information systems or other HHS resources.

(iii) Specific actions and activities are required in certain events—

(A) *Renewal*. A contractor employee's HHS issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be

required to sign-in daily for facility access and may have limited access to information systems and other resources.

(B) *Lost/stolen*. Immediately upon detection, the Contractor or contractor employee must report a lost or stolen HHS ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local servicing security organization. The Contractor must submit an incident report within 48 hours, through the COR or, if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The Contractor must also report a lost or stolen PIV card through the HHS on-line registration system. If the loss or theft is reported by the Contractor to the local police, a copy of the police report must be provided to the COR or Contracting Officer. From the date of notification to HHS, the Contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

(C) *Replacement*. An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

(D) *Surrender of ID cards*. Upon notification that routine access to HHS facilities, sensitive information, information systems or other HHS resources is no longer required, the Contractor must surrender the HHS issued ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization in accordance with agency procedures.

(j) *Flow down of clause*. The Contractor is required to include this clause in any subcontracts at any tier that require the subcontractor or subcontractor's employees to have access to HHS facilities, sensitive information, information systems or other resources.

(End of clause)

## 352.224-70 NOTIFICATION OF SYSTEM OF RECORDS NOTICE (FEB 2024) (DEVIATION)

(a) This contract provides for the design, development, or operation of a system of records about individuals from which information about an individual is retrieved by the individual’s name or by some other identifying particular assigned to the individual.

(b) The System of Records Notice(s) (SORN(s)) that is applicable to this contract is/are: **09-25-0005, Administration: Library Operations and NIH Library User I.D. File and 09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records**.

(c) The System of Records design, development, or operation work the Contractor is to perform is: **The contractor will provide a fully integrated journal submission, manuscript review, and web publishing/hosting platform. This platform will accept submissions from authors, manage a peer-review process, and publish articles. This involves the collection**

**and management of Personally Identifiable Information (PII) including names, email addresses, affiliations, and ORCID iDs for authors, reviewers, and users**

(d) The disposition to be made of the Privacy Act records upon completion of contract performance is as follows: **At the end of contract performance, the contractor will securely transfer all records to the government. The contractor shall not retain any copies of the records. Mailing lists become the property of the U.S. government at the conclusion of the contract.**

(e) *Subcontract flow down*. The Contractor is required to include this clause in all subcontracts at any tier performing work under the prime contract involving design, development, or operation work involving a System of Records.

(End of clause)

## 352.224-71 CONFIDENTIAL INFORMATION (FEB 2024) (DEVIATION)

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

*Confidential information* means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) *Identification of information.* Specific confidential information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, is identified in this contract.

(c) *Disclosure.* The Contractor shall not disclose confidential information or records until written notice is provided to the Contracting Officer at least 45 days in advance of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency. The Contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

(d) *Government furnished or provided information:* For information provided by or on behalf of the government—

(1) The publication or dissemination of the following types of information are restricted under this contract: **Unpublished manuscripts, reviewer comments, and any personally identifiable information (PII) of authors, reviewers, or users beyond what is publicly available in the published articles.**

(2) The reason(s) for restricting the types of information identified in subparagraph (d)(1) is/are: **To protect the integrity of the peer-review process, respect the privacy of individuals involved, and safeguard intellectual property prior to publication.**

(e) The Contractor shall consult with the Contracting Officer when there is uncertainty with regard to the confidentiality of, or a property interest in, information under this contract prior to the release, disclosure, dissemination, or publication of such information.

(End of clause)

## 352.239-71 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2024) (DEVIATION)

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

*Information technology* has the same meaning in FAR 2.101.

*Information and communication technology (ICT) also means* information technology (see FAR 2.101 for definitions).

*Information system security plan* means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) *Responsibilities*. The Contractor shall be responsible for information technology security for all systems connected to a Department of Health and Human Services (HHS) network or operated by the Contractor for HHS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to HHS information that directly supports the mission of HHS. Examples of tasks that require security provisions include—

(1) Hosting of HHS e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by HHS with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to HHS general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) *Information system security plan*. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. HHS information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, privacy impact assessment (PIA), system interconnection agreements, contingency

plan, security configurations, configuration management plan, incident response plan, and the system privacy plan, as determined by the Contracting Officer's Representative. The plan shall address the specific contract requirements regarding information systems or related support or services included in the contract, to include the PWS or SOW. The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information technology security requirements in accordance with Federal and HHS policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following:

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) Federal Information Processing Standard (FIPS) 200; and

(4) HHS Cybersecurity Program related to HHS information (including HHS sensitive information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, the Cyber Security Checklist and Cyber Security Infographic at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html, which provides HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting HHS information, information systems (see 302.101, Definitions), information technology, and ICT, security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.

(d) *Submittal of plan*. Within 60 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) *Authority to Operate (ATO)*. As required by current HHS policy, the Contractor shall submit written proof of information technology security accreditation with a valid ATO to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with HHS policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this ATO a final security plan, risk assessment, security test and evaluation, privacy threshold analysis or privacy impact assessment, and a disaster recovery plan/continuity of operations plan.

(f) *Annual validation*. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.

(g) *Banners*. The Contractor shall ensure that the official HHS banners are displayed on all HHS systems (both public and private) operated by the Contractor that contain Privacy Act or other sensitive information before allowing anyone access to the system. The Office of Information Technology will make official HHS banners available to the Contractor.

(h) *Screening and access*. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for HHS or interconnected to an HHS network in accordance with HHS policies referenced in paragraph (c).

(i) *Training*. The Contractor shall ensure that its employees performing services under this contract complete HHS security awareness and privacy training on an annual basis. This includes signing an acknowledgment on an annual basis that they have read, understand, and agree to abide by the HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy as required; FAR 39.105, Privacy; clause 352.204-71, Information and Information Systems Security, and this clause.

(j) *Government access*. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information systems, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information technology inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of HHS data or to the function of information technology systems operated on behalf of HHS), and to preserve evidence of computer crime.

(k) *Notification of termination of employees*. The Contractor shall immediately notify the Contracting Officer when an employee who has access to HHS information systems or data terminates employment.

(l) *Subcontract flow down requirement*. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

## 352.239-72 INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2024) (DEVIATION)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 352.239-71, Security Requirements for Information Technology Resources.

(End of provision)

## 352.239-73 INFORMATION SYSTEM DESIGN AND DEVELOPMENT (FEB 2024) (DEVIATION)

(a) *Design or development at non-HHS facilities*. Information systems that are designed or developed for or on behalf of HHS at non-HHS facilities shall comply with all HHS directives developed in accordance with the Federal Information Security Modernization Act of 2014, Health Insurance Portability and Accountability Act (HIPAA) regulations, National Institute of

Standards and Technology (NIST), and related HHS security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR Part 164, Subpart C, information and system security categorization level designations in accordance with Federal Information Processing Standards (FIPS) 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections Reference Architecture.

(b) *Privacy Impact Assessment*. During the development cycle a Privacy Impact Assessment must be completed by the contractor, provided to the Contracting Officer Representative, and approved by the appropriate HHS and Operating Division security and privacy officials; government, contractor, or independent third party.

(c) *Security of procured or developed systems and technologies*. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that security fixes shall not negatively impact the Systems.

(d) *Subcontract flow down requirements*. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts where services to perform information system design and development are required.

(End of clause)

## 352.239-74 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE (FEB 2024) (DEVIATION)

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

*Assessment and Authorization* (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable HHS policies and procedures is the mechanism by which HHS provides an Authorization to Operate (ATO), the official management decision given by the HHS to authorize operation of an information system.

*Information system security plan* means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) *Hosting, operation, maintenance, or use at non-HHS facilities*. For information systems that are hosted, operated, maintained, or used on behalf of HHS at non-HHS facilities,

Contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required HHS confidentiality statutes included in HHS mandatory yearly training and privacy policy, Federal Information Security Modernization Act (FISMA), National Institutes of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and HHS security and privacy policy. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security and privacy control procedures must be equivalent to or exceed, those procedures used to secure HHS systems. A Privacy Impact Assessment (PIA) (if the system includes Personally Identifiable Information (PII)) or a Privacy Threshold Analysis (to determine if the system includes PII) must also be provided to the Contracting Officer Representative (COR) and approved by HHS Senior Agency Official for Privacy (SAOP) or designee prior to ATO. All external Internet connections to HHS network involving HHS information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and reviewed and approved by HHS prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) *Collecting, processing, transmitting, and storing of PII*. Adequate security and privacy controls for collecting, processing, transmitting, and storing of PII, as determined by the HHS SAOP or designee, must be in place, tested, and approved by HHS prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of HHS. These security and privacy controls are to be assessed and stated within the PIA, Information System Security Plan, Information System Privacy Plan, Security Control Assessment Report, and/or Privacy Control Assessment Report, as agreed upon by the Contractor, COR, and the Operating Division Senior Official for Privacy. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

(d) *Annual FISMA security controls assessment*. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into HHS Plan of Action & Milestones (POA&M) management process. The Contractor/subcontractor must use HHS POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the HHS in the performance work statement or statement of work, or in the approved remediation plan through the HHS POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by HHS officials, including the HHS Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per HHS

Rules of Behavior for the Use of HHS Information and IT Resources Policy. Major changes introducing new privacy risks require an updated and reapproved PIA.

(e) *Annual self-assessment*. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. HHS reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) *Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on HHS networks*. HHS prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on HHS networks. If non-HHS owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, performance work statement, statement of work, or contract. All of the security controls required for government furnished equipment must also be utilized in approved other equipment (OE) at the Contractor's expense. All remote systems must be equipped with, and use, an HHS-approved antivirus software and a personal (host-based or enclave based) firewall that is configured with an HHS-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-HHS owned OE.

(g) *Disposal or return of electronic storage media on non-HHS leased or non-HHS owned IT equipment*. All electronic storage media used on non-HHS leased or non-HHS owned IT equipment that is used to store, process, or access HHS information must be handled in adherence with disposition instructions upon—

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (*e.g*., hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain HHS information must be returned to the HHS for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per disposition instructions. This must be completed within 30 days of termination of the contract.

(h) *Bio-Medical devices and other equipment or systems*. Bio-Medical devices and other equipment or systems containing media (*e.g.*, hard drives, optical disks) with HHS sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of HHS sensitive information the devices may be provided back to the Contractor under one of three scenarios—

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn-in if HHS initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

## 352.239-75 SECURITY CONTROLS COMPLIANCE TESTING (FEB 2024) (DEVIATION)

On a periodic basis, HHS, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein HHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of HHS, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by HHS in the event of an incident or a breach, or at any other time.

(End of clause)

## 352.239-76 SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED CONTRACTOR-OPERATED AND CONTRACTOR-OWNED CONTRACTOR-OPERATED RESOURCES (FEB 2024) (DEVIATION)

(a) *Federal policies*. The Contractor shall comply with applicable federal laws, regulations, and HHS policies that include, but are not limited to—

(1) HHS Policy for Information Security and Privacy Protection (IS2P);

(2) Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101);

(3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, Security and Privacy Controls for Information Systems and Organizations;

(4) Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and

(5) Any other applicable federal laws, regulations, NIST guidance, and local HHS policies.

(b) *Assessment and Authorization (A&A).* A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) of **within the specified timeline(s) of 180 days after contract award**. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P*, NIST SP 800-37,

*Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision). HHS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

(1) *A&A package deliverables.* The Contractor shall provide an A&A package within **120 days after contract award** to the Contracting Officer and/or the Contracting Officer's Representative (COR). The following A&A deliverables are required to complete the A&A package—

(i) **System Security Plan (SSP), Security Assessment Plan/Report (SAP/SAR), Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA), System Privacy Plan and Privacy Control Assessment, Independent Assessment, Plan of Actions and Milestones (POA&M), Contingency Plan and Contingency Plan Test, and E-Authentication Questionnaire**:

(ii) A System Security Plan (SSP) is due **120 days after contract award.** The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system (see HHSAR 302.101, Definitions) as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall review and update the SSP at least annually thereafter and if requested, provide a copy of the updated SSP to the COR.

(iii) A Security Assessment Plan/Report (SAP/SAR) is due **120 days after contract award**. The security assessment must be conducted by the assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with the COR shall conduct, or as directed, in the assessment of the security controls and update the SAR at least annually. A copy of the updated SAR shall be provided to the COR, if requested.

(iv) All systems shall have a completed privacy threshold analysis (PTA). If the PTA results determines the system contains personally identifiable information, a privacy impact assessment, approved by the HHS SAOP, is required.

(v) System Privacy Plan and Privacy Control Assessment. As required in OMB Circular A-130, a System Privacy Plan and Privacy Control Assessment shall be included in A&A. The plan and assessment may be included in the Security System Plan, or a separate report in the A&A, as determined by the COR.

(vi) An Independent Assessment is due **120 days after contract award**. The Contractor shall have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party shall review and analyze the security authorization package and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all *"high"* deficiencies **and criticals** before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).

(vii) The POA&M is due as follows—

(A) **Within 30 days** from the date the weaknesses are formally identified and documented;

(B) Critical-risk weaknesses must be mitigated within **15 days** from the date the weaknesses are formally identified and documented;

(C) High-risk weaknesses must be mitigated within **30 days**from the date the weaknesses are formally identified and documented;

(D) Medium weaknesses must be mitigated within **90 days**from the date the weaknesses are formally identified and documented; and

(E) Low weaknesses must be mitigated within **180 days**, from the date the weaknesses are formally identified and documented.

(2) HHS will determine the risk rating of all vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones policies. Depending on the severity of the risks, HHS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document shall be updated at least quarterly **and upon mitigation of any weakness**.

(3) A Contingency Plan and Contingency Plan Test are due **120 days after contract award**. The Contingency Plan shall be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS policies. Upon final acceptance by the System Owner, the Contractor, in coordination with the COR and System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned, and any remaining action items to be addressed. The Contractor shall update and test the Contingency Plan at least *annually*.

(4) An E-Authentication Questionnaire is required. The Contractor shall collaborate with at the COR's direction to ensure that the E-Authentication Guidance requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 series, latest versions. Based on the level of assurance determined by the E-Authentication, the Contractor shall ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Authentication (when required), in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS policies.

(5) *Information security continuous monitoring.* Upon the government issuance of an ATO, the Contractor-owned/operated systems that input, store, process, output, and/or transmit government information shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, and HHS IS2P.

(6) *Annual assessment/penetration (pen) test*. The Contractor shall assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by the specified due date provided by the COR.

(7) *Asset management.* Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, the Contractor shall provide an inventory of all information technology (IT) assets for hardware and software (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information and/or data. It is anticipated that this inventory information will be required to be produced at least **annually**. IT asset inventory information shall include—

(i) IP address;

(ii) Machine name;

(iii) Operating system level;

(iv) Security patch level; and

(v) SCAP-compliant format information. The Contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.

(8) *Configuration management*. The Contractor shall use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to computers, servers, routers,

databases, operating systems, application, etc., that store and process government information. The Contractor shall provide scan reports to the COR upon request. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

(9) *Vulnerability management.* The Contractor shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least **monthly**.

(10) *Patching and vulnerability remediation*. The Contractor shall install vendor-released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

(11) *Secure coding.* The Contractor shall follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team specified standards, the Software Engineering Institute (SEI) CERT and the Open Web Application Security Project, that will limit system software vulnerability exploits.

(12) *Boundary protection.* The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection.

(13) *Government access for security assessment*.

(i) In addition to the Inspection Clause in the contract, the Contractor shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS. This access includes, but is not limited to—

(1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, access to Contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. For the purposes of this paragraph only, *Government* includes, but is not limited to, Contracting Officer, COR, the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The

purpose of access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include, but not be limited to, such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, Structured Query Language injection vulnerabilities, and any other known vulnerabilities.

(2) At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

(ii) The Contractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Government inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

(iii) The Contractor shall cooperate with inspections, audits, investigations, and reviews.

(c) *End of Life compliance*. The Contractor shall use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the OPDIV CISO if it impacts only the OPDIV). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.

(d) *Desktops, laptops, and other computing devices required for use by the Contractor.* The Contractor shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

(1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program.

(2) Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline, **and NIH**, and HHS Minimum Security Configuration Standards;

(3) Maintain the latest operating system patch release and anti-virus software definitions at least **weekly**;

(4) Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

(5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

(i) Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

(ii) Using SCAP-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the Contracting Officer and/or COR, Project Officer, and any other point of contract designated by the Contracting Officer or COR.

(e) *Rights to data.* Contractors shall specify any data rights asserted and mark such deliverables accordingly in accordance with applicable data rights clauses set forth in the contract.

(f) *Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements*. The Contractor shall secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232, section 889. At a minimum, the Contractor shall—

(1) Develop rules for suppliers' development methods, techniques, or practices;

(2) Use secondary market components;

(3) Prohibit counterfeit products;

(4) Dispose and/or retain elements such as components, data, or intellectual property securely;

(5) Ensure adequate supply of components;

(6) Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;

(7) Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;

(8) Establish Service Level Agreements (SLAs), patching vehicles, and disclosure requirements in the case of an incident or new vulnerability being discovered; and

(9) Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and

(10) Prohibit the use of covered telecommunications and video surveillance equipment or services.

(g) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts and third-party agreements, at any tier, of any amount and in which subcontractor employees and third-party servicers/employees, will perform functions or provide products under the scope of this contract, and have access to HHS information (including HHS sensitive information, *i.e.*, protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101, Definitions).

(End of clause)

## 352.239-77 CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION)

(a) *Responsibilities.* This clause is applicable to all or any part of the contract that includes cloud computing services. The Contractor shall be responsible for the following privacy and security requirements on this contract—

(1) *Federal Risk and Authorization Management Program (FedRAMP) compliant authorization to operate.* Compliance with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service (see HHSAR 302.101, Definitions) under this contract has an approved FedRAMP compliant authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by **leveraging an active, existing FedRAMP Moderate Authorization (Joint Authorization Board (JAB) or another Federal Agency), unless an NIH Agency Sponsorship is explicitly directed and approved by the NIH Authorizing Official (AO). The Contractor's plan for achieving this ATO must be submitted by 60 days after contract award**.

(i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at fedramp.gov). The *HHS Policy for Information Security and Privacy Protection*

*(IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall implement additional controls identified by the agency in this contract.

(ii) A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter, or when there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

(2) *Data jurisdiction.* The Contractor shall store all information within the security authorization boundary, data at rest, or data backup, within the Continental United States, when applicable.

(3) *Service Level Agreements (SLAs)*. When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and the cloud service provider and work with the Contracting Officer's Representative (COR) to develop and maintain an SLA, as provided in the contract.

(4) *Interconnection Agreements/Memorandum of Agreements.* When applicable and identified in this contract, the Contractor shall establish and maintain interconnection agreements and or memorandum of agreements/understanding in accordance with HHS policies.

(b) *Protection of information in a cloud environment.*

(1) If Contractor personnel shall remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS policies, available at https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html.

(2) HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data shall be made available to HHS, at no additional cost, within one (1) business day from the date of the request, or within the timeframe otherwise specified.

(3) The Contractor shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

(4) The Contractor shall comply with NARA-approved records schedule(s) and protection requirements for federal agency electronic records in accordance with 36 CFR 1236.20 and 1236.22 (ref. a), including but not limited to —

(i) Maintenance of links between records and metadata; and

(ii) Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

(5) The disposition of all HHS data shall be at the written direction of the COR. This may include documents returned to HHS control, destroyed, or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(i) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the **Privacy Act requirements in the contract.**

(c) *Assessment and Authorization (A&A) process*.

(1) The Contractor shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, privacy policies, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS security policies.

**The Contractor shall submit a complete, high-quality Leveraged A&A package within 120 days of award, with the goal of achieving a signed NIH Leveraged ATO within 180 days of award**.

(i) In addition to the FedRAMP compliant ATO, the Contractor shall complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation **and annually thereafter.** The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.

(ii) Cloud Service Provider (CSP) systems categorized as FIPS 199 High, Moderate or Low are recommended but not required to leverage a FedRAMP accredited Third Party Assessment Organization (3PAO). A CSP's agency partner may choose to use their own Independent Verification and Validation (IV&V) organization or 3PAO to assess the system. If an agency chooses to use their own IV&V team or an unaccredited 3PAO, they must submit an attestation regarding the team's independence to the agency and the FedRAMP PMO, and the IV&V / 3PAO team must use FedRAMP templates for the assessment and follow all FedRAMP requirements.

(iii) For all cloud services, the A&A package must contain the following documentation:

**Active FedRAMP Moderate Package (including SSP, SAR, and POA&M) shared via the FedRAMP Package Access Request form, NIH-specific Privacy Impact Assessment (PIA), and NIH Leveraged ATO template.**

(iv) Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with HHS policies. The following templates and timelines are applicable.

**Deliverables are due within the timelines specified in HHSAR clause 352.239-76**.

(2) HHS reserves the right to perform penetration testing on all systems operated on behalf of the agency. If the Contracting Officer exercises this right, the Contractor shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to—

(i) Scanning operating systems, web applications, wireless scanning;

(ii) Network device scanning to include routers, switches, and firewall, and IDS/IPS; and,

(iii) Databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

(3) The Contractor shall identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the Contractor's expense before HHS issues an ATO.

(4) The Contractor shall mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings shall be remediated in accordance with timelines specified in the HHS POA&M Standard from discovery—

(i) Critical vulnerabilities no later than fifteen (15) days;

(ii) High within thirty (30) days;

(iii) Medium within ninety (90) days; and

(iv) Low vulnerabilities no later than three hundred and sixty (360) days, unless otherwise specified.

(v) In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines **14 days**. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

(5) Revocation of a cloud service. HHS has the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information (see HHSAR 302.101, Definitions), HHS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the internet, other networks, or applying additional security controls.

(d) *Reporting and continuous monitoring.*

(1) Following the initial ATOs, the Contractor shall perform the minimum ongoing continuous monitoring activities, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. The minimum ongoing continuous monitoring activities include—

**See contract and PWS deliverables – as applicable.**

(2) At a minimum, the Contractor shall provide the following artifacts/deliverables on a monthly basis—

**See contract and PWS deliverables – as applicable.**

(i) Operating system, database, Web application, and network vulnerability scan results;

(ii) Updated POA&Ms;

(iii)Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO, and;

(iv) Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract shall be approved by the agency.

(e) *Configuration baseline*.

(1) The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of

software must not alter the configuration settings from the approved HHS **and NIH** configuration baseline.

(2) The Contractor shall use NIST Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

(f) *Report of known or suspected incident or breach*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of an known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than **30** days. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (*e.g.*, Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within **the timelines specified in the HHS and NIH Policies for Vulnerability Management**.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–- Security and Privacy Language.

(g) *Incident and breach investigation*. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(h) *Incident and breach notification requirements*. (1) The Contractor/subcontractor shall provide notice to HHS of a privacy or incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third-party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(i) *Media transport*.

(1) The Contractor shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

**All portable media must be encrypted using FIPS 140-validated encryption**.

(2) All information, devices and media shall be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

(j) *Boundary Protection—Trusted Internet Connections (TIC).*

(1) The Contractor shall ensure that government information (other than unrestricted information) being transmitted from Federal government entities to external entities using cloud services is inspected by TIC processes that are in compliance with the requirements of the Office of Management and Budget Memorandum 19-26: Update to the TIC Initiative, TIC 3.0.

(2) The Contractor shall route all external connections through a TIC.

(3) Non-Repudiation. The Contractor shall provide a system that implements encryption with current FIPS 140 validation certificate from the NIST Cryptographic Module

Validation Program that provides for origin authentication, data integrity, and signer non-repudiation.

(k) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (i), in subcontracts and third-party agreements, of any amount and in which subcontractor employees, and third-party servicers/employees, will perform functions where they will provide cloud computing services and have access to HHS information (including HHS sensitive information, *i.e.*, protected health information (see HHSAR 302.101, Definitions)), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts).

(End of clause)

## 352.239-78 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2024) (DEVIATION)

(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.

(c) If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(d) In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the

requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available at https://Section508.gov/.

(e) In order to facilitate the Government's determination whether proposed ICT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(f) Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(g) Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

(End of provision)

## 352.239-79 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2024) (DEVIATION)

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) Additional Section 508 accessibility standards applicable to this contract or order may be identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an ACR (based on the VPAT see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements.

(End of clause)