H.14 Encryption Language and Security Requirements for Federal Information Technology Resources

1.A Baseline Security Requirements

1.A.1 Applicability. **The following requirements apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:**

1. Access (Physical or Logical) to Federal Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, physical or logical (electronic) access to federal information.

2. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that directly supports the HHS mission. In addition to the FAR Subpart 2.1 definition of "information technology" (IT), the term as used in this section, includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources. This section does not apply to national security systems as defined by the Federal Information Security Modernization Act (FISMA) of 2014.

1.A.2 Safeguarding Information and Information Systems. The Contractor (and/or any subcontractor) is responsible for the following:

1. On behalf of HHS and DCAS, protecting federal information and information systems in order to ensure:
   a. **Confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
   b. **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
   c. **Availability**, which means ensuring timely and reliable access to and use of information.
2. Providing security of any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location per clause 52.239-1 of the Federal Acquisition Regulation (FAR) (https://www.acquisition.gov/sites/default/files/current/far/html/52_233_240.html).
   a. The Contractor is prohibited from subcontracting to companies to conduct HHS business in which foreign governments that support international terrorism have a "significant interest" per 10 U.S.C. § 2327 (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/html/USCODE-2011-title10-subtitleA-partIV-chap137-sec2327.htm).
3. Adopting, and implementing, at a minimum, the policies, procedures, controls, and standards required by HHS Information Security Program to ensure the confidentiality, integrity,, and availability of federal information and federal information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. The HHS Information Security Program security requirements are outlined in the HHS IS2P, which is accessible on the HHS Office of the Chief Information Officer's (OCIO) website (http://intranet.hhs.gov/it/ocio/).
   a. The Information Security Solicitation Checklist and Certification Form (See Appendix A, for the Information Security Solicitation Checklist and Certification Form) must be completed when the acquisition requires contractor personnel to develop or access federal information systems.

1.A.3. Information Security Categorization. The Contractor/subcontractor will coordinate with the system owner, Contracting Officer Representative (COR) and/or Contracting Officer to categorize the system and information to determine applicable information type(s) and the overall level of risk

in accordance with FIPS-199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) and the *Federal Information Processing Standard* NIST SP 800-60, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories", Appendix C, Table C-2 at Vol 2 (http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf). The security categories and risk level shall be documented in the designated System Security Plan (SSP).

1.A.4. Internet Protocol Version 6 (IPv6). All acquisitions using Internet Protocol must comply with FAR sections: FAR 7.105(b)4, FAR 11.002(g), and FAR 12.202(e) (https://www.acquisition.gov/?q=browsefar).

1.A.5. Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a federal information system(s). The roster shall be submitted to the Contracting Officer's Representative (COR), with a copy to the Contracting Officer, within *14 days* of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within *14 days* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

1.A.6. Contract Documentation. The Contractor shall contact the Contracting Officer and/or COR for any *[DCAS Specific]* templates, policies, forms and other documents necessary to comply with the requirements of this section. All contract deliverables shall be compliant with Section 508.

1.A.7. Standard for Encryption

1. The Contractor (and/or any subcontractor) shall comply with the *HHS Standard for Encryption Language in HHS Contracts* (http://www.hhs.gov/ocio/policy/2009-0002.001s.html) to prevent unauthorized access to HHS information.

2. The Contractor (and/or any subcontractor) shall use FIPS 140-2, Security Requirements for Cryptographic Module (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) compliant encryption to protect all instances of HHS sensitive information during storage and transmission

*(**NOTE**: The HHS Standard for the Definition of Sensitive Information (http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/HM/dept_standard_for_def_of_sens_info-051809.pdf), latest revision, must be used to determine if information under this contract is sensitive).*

3. The Contractor (and/or any subcontractor) shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (http://csrc.nist.gov/groups/STM/cmvp/) to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR and/or Contracting Officer.

4. The Contractor (and/or any subcontractor) shall use the Key Management Key (http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf) on the HHS personal identification verification (PIV) card; or alternatively, the Contractor (and/or any subcontractor) shall establish and use a key recovery mechanism to ensure the ability for authorized personnel to decrypt and recover all encrypted information (OMB Encryption Guidance at http://csrc.nist.gov/drivers/documents/ombencryption-guidance.pdf). The Contractor shall notify the COR and/or Contracting Officer of personnel authorized to decrypt and recover all encrypted information.

5. The Contractor (and/or any subcontractor) shall ensure that HHS and DCAS specific encryption standard is incorporated into the Contractor's property management/control system or establish a separate procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive HHS information (including PII).

6. The Contractor (and/or any subcontractor) shall ensure that encryption keys are provided to the COR and/or Contracting Officer upon request and at the conclusion of the contract.

1.A.8. Protection of Sensitive Information. All federal information that may be sensitive (as defined in the Departmental Standard for the Definition of Sensitive Information) shall be protected in accordance with Office of Management and Budget (OMB) Memorandum (M) 06-16 (https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf), Protection of Sensitive Agency Information and encrypted with Federal Information Processing Standard (FIPS) 140-2 compliant solution.

1.A.9. Contractor Agreement. The Contractor (and/or any subcontractor), performing under this contract, shall not release, publish, or disclose non-public[1] federal information to unauthorized individuals. The confidentiality, integrity, and availability of such information shall be protected by the Contractor in accordance with the governing laws and regulations listed as follows:
- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records) (https://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap31-sec641/content-detail.html)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information) (https://www.gpo.gov/fdsys/pkg/USCODE-2014-title18/pdf/USCODE-2014-title18-partI-chap93-sec1905.pdf)
- Public Law 96-511 (Paperwork Reduction Act) (http://ciog6.army.mil/Portals/1/Policy/PaperReduction 1980.pdf)

1.A.10. Contractor Employee Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public federal information under this contract shall complete the DCAS Commitment to Protect Non-Public Information – Contractor Employee Agreement. *[DCAS inserted information/link should be cited here]*, as applicable. A copy of each signed and witnessed NDA shall be submitted to the COR and/or Contracting Officer prior to performing any work under this acquisition (See Appendix C for the HHS Contractor Non-Disclosure Agreement).

1.A 11. Privacy or Security Safeguards (FAR Clause 48 CFR § 52.239-1).

1. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

3. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

1.A.12. Confidential Information (HHSAR Clause 48 CFR § 352.224-71).

[1] "Non-public" in this document refers to information only to be used by authorized individuals including authorized contractors.

1. Confidential Information, as used in this clause, 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.

2. Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this contract. The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.

3. Confidential Information or records shall not be disclosed by the Contractor until:

   a. Written advance notice of at least ***45 days*** shall be provided to the Contracting Officer 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.

   b. For information provided by or on behalf of the government,

      i. The publication or dissemination of the following types of information are restricted under this contract: *NONE*

      ii. The reason(s) for restricting the types of information identified in subparagraph (i) is/are: None

   c. Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

   d. Whenever the Contractor is uncertain with deciding if information is confidential under this contract, the Contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication of that information.

1.A.13. Privacy Threshold Analysis (PTA)[2] – due within *45 days* after contract award.

1. The Contractor shall assist the Senior Agency Official for Privacy (SAOP) (or his or her designee)[3] with conducting a PTA (using the Privacy Impact Assessment [PIA] form) for the information system and/or information collection project to determine whether or not a full PIA needs to be completed.

   a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the SAOP (or his or her designee) and other designated authorities with completing a PIA for the system or project within *30 days* after completion of the PTA.

   b. The PIA shall be completed in accordance with HHS policy, OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (https://www.whitehouse.gov/omb/memoranda_m03-22) and shall be revised at each milestone during the system development lifecycle (SDLC).

[2] At HHS, the same form (i.e., the PIA form) is used for both the Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA). More questions on the form must be answered when the threshold answers indicate PII is involved.

[3] HHS Privacy Officers are listed here: http://intranet.hhs.gov/it/cybersecurity/privacy/#header1. Some of them may also be HHS Privacy Act Contacts, mentioned in Section 3.

c. PIAs must be reviewed at least ***annually*** and whenever a significant change is made to the information systems or when new PII is collected, that introduces new or increased privacy risks.

1.B. Training

1.B.1. Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees shall complete the applicable DCAS Information Security Awareness, Privacy, and Records Management training *before performing any work under this contract*. Thereafter, the employees shall complete DCAS specified Information Security Awareness, Privacy, and Records Management training *at least annually*, during the life of this contract. All Contractor/subcontractor provided training shall be compliant with HHS training policies.

1.B.2. Role-based Training. HHS requires role-based training when responsibilities associated with a given role or position, could, upon execution, have the potential to adversely impact the security posture of one or more HHS systems and information. The *HHS Memorandum on Role-Based Training Requirement* (http://intranet.hhs.gov/it/cybersecurity/policies/index.html) provides further guidance on the user roles that have significant security responsibilities.

1.B.3. Training Records. The Contractor (and/or any subcontractor) shall maintain training records for all information security and privacy training completed by all of its employees working under this contract, taken outside the Department and/or DCAS training system. The training records shall be provided to the COR and/or Contracting Officer in conjunction with contract award[4] or upon request and any DCAS specific rules as applicable. The Contractor shall provide records of any applicable information security and privacy training completed outside of HHS/DCAS to the COR and/or Contracting Officer responsible for their contract.

1.C Rules of Behavior

1.C.1. The Contractor (and/or any subcontractor) shall ensure that all employees comply with the HHS Information Technology General Rules of Behavior (http://intranet.hhs.gov/it/cybersecurity/policies/index.html), and any DCAS specific rules, as applicable.

1.C.2. All Contractor employees must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process HHS information initially and at least ***annually*** thereafter, which may be done as part of annual DCAS Information Security Awareness Training.

1.D Incident Response

1.D.1. Per FAR 52.239-1, if new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

1.D.2. The Contractor (and/or any subcontractor) shall report all suspected and confirmed information security and privacy incidents to the DCAS IRT, COR, Contract Officer, SAOP (or his or her designee), and other stakeholders, including incidents involving personally identifiable information (PII), in electronic or physical form, within ***1 hour*** of discovery. The types of information required in a cyber-incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised.

[4] This training information must be available for the COR and/or the Contracting Officer before contractors (and subcontractors) start performing any work under this contract.

1.D.3. In the event of an information security or privacy incident, the Government may suspend or revoke an existing authority to operate (ATO) (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor (and/or any subcontractor) to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor (and/or any subcontractor) IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

1.D.4. The Contractor (and/or any subcontractor) shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. Incident response activities determined to be required by the Government may include, but are not limited to, the following:

1. Inspections,
2. Investigations,
3. Forensic reviews, and
4. Data analysis and processing.

1.E Position Sensitivity Designations

1.E.1. All Contractor (and/or any subcontractor) employees must obtain a security clearance commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR) (https://www.opm.gov/investigations/background-investigations/position-designation-tool/). The following position sensitivity designations apply to this contract:

[ ] Level 6: Public Trust - High Risk. Contractor (and/or any subcontractor) employees assigned to Level 6 positions shall undergo a Suitability Determination and Background Investigation (BI).

[X] Level 5: Public Trust - Moderate Risk. Contractor (and/or any subcontractor) employees assigned to Level 5 positions with no previous investigation and approval shall undergo a Suitability Determination and a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI).

[ ] Level 4: Special Sensitive. Contractor (and/or any subcontractor) employees assigned to Level 4 positions with no previous investigation and approval shall undergo a Suitability Determination and a Single Scope Background Investigation (SSBI),

[ ] Level 3: Top Secret – Critical Sensitive. Contractor (and/or any subcontractor) employees assigned to Level 3 positions with no previous investigation and approval shall undergo a Suitability Determination and Single Scope Background Investigation (SSBI),

[ ] Level 2: Confidential or Secret – Noncritical Sensitive. Contractor (and/or any subcontractor) employees assigned to Level 2 positions with no previous investigation and approval shall undergo a Suitability Determination and a Access National Agency Check, Inquiries (ANACI)

[X] Level 1: Non-Sensitive Contractor (and/or any subcontractor) employees assigned to Level 1 positions shall undergo a Suitability Determination and National Agency Check and Inquiry Investigation (NACI).

1.E.2. All Contractor (and/or any subcontractor) employees shall comply with the conditions established for their designated position sensitivity levels prior to performing any work under this contract (See Appendix A).

1.E.3. Suitability Investigations are required for contractors (and/or any subcontractor) who will need access to federal information systems and/or to federally controlled physical space.

1.F Personnel Security Responsibilities

1.F.1. The Contractor, within *[DCAS specific timeline]* before an employee begins working on this contract, shall provide the COR and/or Contracting Officer, and Information System Security Officer (ISSO) the name, position title, e-mail address, and phone number of all contract employees working under the contract per the National Industrial Security Program Operating Manual (NISPOM) Section 2-200 (http://intranet.hhs.gov/security/ossi/documents/nispom.pdf), the HHS Contract Closeout Guide (2012) (http://intranet.hhs.gov/abouthhs/contracts-grants-support/acquisition-policies-guidance/acquisition-worktools/contract-closeout-tableofcontents/), and the HHS Personnel Security & Suitability Policy, Section 7.6 (http://intranet.hhs.gov/security/ossi/documents/pssp.pdf).

1. If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.
2. If the employee is filling an existing position, the Contractor shall provide the name, position title and suitability determination level held by the former incumbent.

1.F.2. The Contractor shall notify the COR and/or Contracting Officer and system ISSO within 14 days before an employee stops working under this contract.

1. The Contractor shall provide the name, position title, and suitability determination level held by or pending for departing employees to the COR and/or Contracting Officer.
2. The Government will stop pending background investigations for employees that no longer work under this acquisition.

1.F.3. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the Contractor Employee Separation Checklist when a Contractor (and/or any subcontractor) employee terminates work under this contract. All documentation shall be made available to the COR and/or Contracting Officer upon request.

1.F.4. Within *5 days* after the Government's final acceptance of the work under this contract, or upon termination of the contract, the Contractor shall return all identification badges to the Contracting Officer or designee.

1.G Homeland Security Presidential Directive (HSPD)-12

1.G.1. To gain routine physical access to an HHS facility, logical access to an HHS-controlled information system, and/or access to sensitive data or information, the Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; Office of Management and Budget (OMB) Memorandum (M)05-24; and Federal Information Processing Standards Publication (FIPS PUB) Number 201, Federal Acquisition Regulation (FAR) Subpart 4.13 (https://www.acquisition.gov/sites/default/files/current/far/html/Subpart 4_13.html), FAR Subpart 52.204-9 (https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf); and with the personal identity verification and investigation procedures contained in the following documents:

1. HHS *Information Security and Privacy Policy (IS2P)* (http://intranet.hhs.gov/it/cybersecurity/policies/index.html)
2. HHS *Personnel Security and Suitability Policy*

(http://intranet.hhs.gov/security/ossi/documents/pssp.pdf).

3. HSPD-12 *Implementation Policy for the Use of the Personal Identity Verification (PIV) Card for Strong Authentication* (http://intranet.hhs.gov/security/ossi/hspd-12/implementation-policy.html).

1.G.2. This includes foreign national Contractor/subcontractor employees that perform work under this acquisition and meet the requirements to complete a NACI background investigation as residents of the United States for three (3) or more of the last five (5) years (http://intranet.hhs.gov/security/ossi/hspd-12/implementation-policy.html).

1.H Fingerprinting

1.H.1. All Contractor (including any subcontractor) employees must be fingerprinted before gaining access to HHS-controlled information systems in compliance with FAR Subpart 52.204-2 Security Requirements (including Alternate II) (https://www.acquisition.gov/?q=/browse/far/52).

1.H.2. To gain logical access to HHS-controlled information systems, contract employees working under the contract are subject to a fingerprint check.

1.H.3. If a Contractor (and/or any subcontractor) must appear at an HHS facility to be fingerprinted, any costs associated with getting to that facility are to be borne by the Contractor.

1.I Background Investigations

1.I.1. All Contractor (including any subcontractor) personnel must complete a background investigation based on the position designation and type of investigation required as determined by the agency in compliance with FAR Part 52.222-54 -- Employment Eligibility Verification (https://www.acquisition.gov/?q=/browse/far/52) and FAR Subpart 22.18—Employment Eligibility Verification (https://www.acquisition.gov/?q=/browse/far/22).

1.I.2. Based upon information provided by the Contracting Officer (CO)/COR, the Contracting Officer shall insert references to DCAS and/or local procedural guideline(s), if any; indicate if they are readily accessible to the public; and, if so, specify where they may be found. If they are not readily accessible, the Contracting Officer shall attach a copy to the solicitation and contract and reference the guideline(s) here.

1.I.3. At the time of solicitation, based upon information provided by the CO/COR, the Contracting Officer shall specify all known levels. If the position sensitivity levels are not known at that time, the Contracting Officer shall insert the words “To Be Determined at the Time of Award.” However, the Contracting Officer must include the definitive position sensitivity levels in the awarded contract/order.

1.I.4. The personnel investigation procedures for Contractor personnel (and/or any subcontractor) require that the Contractor (and/or any subcontractor) prepare and submit background check/investigation forms based on the type of investigation required. The minimum Government investigation for a non-sensitive position is a National Agency Check and Inquiries (NACI) with fingerprinting. More restricted positions – i.e., those above non-sensitive, require more extensive documentation and investigation.

1. The Contractor shall notify the CO/COR of its proposed personnel who will be subject to a background check/investigation.

2. The Contractor shall notify the CO/COR whether any of its proposed personnel who will work under the contract have previously been the subject of national agency checks or background investigations.

1.I.5. Investigations are expansive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with the FAR section, Excusable Delays – see FAR 52.249-14, if applicable (https://www.acquisition.gov/sites/default/files/current/far/html/52_248_253.html).

1. The Contractor shall ensure that the employees it proposes for work under this contract have a reasonable chance for approval.

1.I.6. The Government may investigate personnel at no cost to the Contractor. However, multiple investigations for the same position may, at the Contracting Officer's discretion, justify reduction(s) in the contract price of no more than the cost of the additional investigation(s).

1.K Audit Record Retention

1.K.1. The Contractor (and/or any subcontractor) shall support a system in accordance with the requirement for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 (http://www.gpo.gov/fdsys/granule/CFR-2011-title36-vol3/CFR-2011-title36-vol3-sec1236-20) & 1236.22 (http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36:3.0.10.2.25) (ref. a), including but not limited to capabilities such as those identified in:

1. NARA Bulletin 2013-02, August 29, 2013, *Guidance on a New Approach to Managing Email Records* (https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html),
2. NARA Bulletin 2010-05 September 08, 2010 (http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html), *Guidance on Managing Records in Cloud Computing Environments* (ref 8).

These provide requirements for maintaining records to retain functionality and integrity throughout the records' full lifecycle including:

1. Maintenance of links between records and metadata, and
2. 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.

2.A Privacy Incident Handling and Notification

The Contractor (and/or any subcontractor) shall obtain notification instructions and approval from the Contracting Officer prior to notifying individuals whose PII resided in the Contractor (and/or any subcontractor) IT system at the time of the incident. The method and content of any notification by the Contractor shall be compliant with HHS Privacy Incident Response Team (PIRT) Standard Operating Procedures (SOP) (http://intranet.hhs.gov/it/cybersecurity/docs/incident_mgmt/PIRTSOP/pirt_sop.pdf) and *[DCAS]* Guidance as well as coordinated and approved by HHS PIRT in consultation with the Contracting Officer, the *[DCAS]* SAOP (or his or her designee), and/or CSIRT. Upon receiving notification and approval from the agency Contracting Officer, the Contractor shall send notifications to affected individuals within *[DCAS Specific timeline]*.

2.A.1. All determinations related to privacy incidents, including response activities, notifications to affected individuals and/or federal agencies, and related services (e.g., credit monitoring and identity protection) will be made in writing by the Contracting Officer in consultation with the HHS PIRT, CIO, and SAOP (or his or her designee) and in compliance with HHS and/or DCAS Guidance.

2.A.2. The Contractor (and/or any subcontractor) shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. Incident response activities determined to be required by the Government may include, but are not limited to, the following:

1. Inspections,
2. Investigations,
3. Forensic reviews, and
4. Data analysis and processing.

2.B Privacy Plan

The Contractor shall submit a plan with its technical proposal, in accordance with the HHS IS2P, that safeguards data and protects the confidentiality of PII (NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf and NIST SP 800-53, Revision 4,, Appendix J http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf); the plan shall:

- Verify the information categorization to ensure the identification of the PII requiring protection.
- Verify the existing risk assessment.
- Identify the Contractor's existing internal corporate policy that addresses the information protection requirements of the SOW.
- Verify the adequacy of the Contractor's existing internal corporate policy that addresses the information protection requirements of the SOW.
- Identify any revisions, or development, of an internal corporate policy to adequately address the information protection requirements of the SOW.
- For PII to be physically transported to or stored at a remote site, verify that the security and privacy controls of NIST Special Publication 800-53, latest version, involving the encryption of transported information will be implemented.
- When applicable, verify how the NIST Special Publication 800-53, latest version, security and privacy controls requiring authentication, virtual private network (VPN) connections and other technical safeguards will be implemented.
- When applicable, verify how the NIST Special Publication 800-53, latest version, security controls enforcing allowed downloading of PII will be implemented.
- Identify measures to ensure subcontractor compliance with safeguarding PII and security and privacy controls in the NIST 800-53.
- Be commensurate with the size and complexity of the contract requirements based on the System Categorization specified above in the subparagraph entitled Security Categories and Levels.
- Be evaluated by the Government for appropriateness and adequacy.

2.C Privacy Act

2.C.1. Privacy Act Notification (FAR Clause 48 CFR § 52.224-1). The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of Section (i) of the Act may involve the imposition of criminal penalties.

2.C.2. Privacy Act (FAR Clause 48 CFR § 52.224-2). The Contractor agrees to—

1. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

    a. The systems of records;

    b. The design, development, or operational work that the contractor is to perform.

2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

    a. Include this clause, including this paragraph, in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

        i. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of Section (i) of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

3. "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

4. "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

5. "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

2.C.3. Privacy Act (HHSAR Clause 48 CFR §352.224-70). This contract requires the Contractor to perform one or more of the following: design; develop; or operate a Federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) (5 U.S.C. 552a(m)(1)) and applicable agency regulations.

1. The term system of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties (5 U.S.C. 552a(i)).

2. The Contractor shall ensure that each of its employees knows the prescribed rules of conduct in 45 CFR part 5b and that each employee is aware that he/she is subject to criminal penalties for violation of Section (i) of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under

this contract which require the design, development or operation of the designated system(s) of records (5 U.S.C. 552a(m)(1)). The contract work statement:

a. Identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and

b. Specifies the disposition to be made of such records upon completion of contract performance.

c. Specifies the use of a disclosure statement (required by Section (e)(3) of the Privacy Act of 1974, as amended) to appear on documents used to PII from individuals to be maintained in a Privacy Act System of Records (SORN).

3.A Security Requirements for GOCO and COCO Resources

3.A.1. Contractor Security Deliverables. In accordance with the timeframes specified, the Contractor shall prepare and submit the following security requirements to the COR and/or Contracting Officer and System Owner or designated representative for review, comment, and acceptance, when applicable and identified in the deliverables section of the contract. All deliverables shall comply with applicable federal laws that include, but are not limited to, the Federal Information Security Modernization Act (FISMA) of 2014, (Title III of the E-Government Act of 2002, Public Law 107-347), Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, Federal Acquisition Regulation (FAR) 39.101 (https://www.acquisition.gov/?q=/browse/far/39), HHS Acquisition Regulation (HHSAR) Subpart 311.70—Section 508 Accessibility Standards (http://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/subpart311/index.html#Subpart311.70--Section508AccessibilityStandards), and other applicable federal laws, regulations, NIST guidance and Departmental policies.

3.A.2. Security Assessment and Authorization (SA&A) – due within *[insert contract specific timeline]* after contract award. The Contractor shall submit written proof to the COR and/or the Contracting Officer that a SA&A was performed for the applicable information system and the system has a valid authority to operate (ATO) that is acceptable to the COR and/or the Contracting Officer. If a SA&A has not been performed, the Contractor (and/or any subcontractor) shall perform the SA&A in accordance with the Office of the Chief Information Officer (OCIO), HHS-OCIO Policy for Information Systems Security and Privacy Policy (IS2P); NIST SP 800-37, latest revision, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and other applicable guidance and acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

1. SA&A Package Deliverables - The Contractor shall include at a minimum the following SA&A deliverables in addition to the PTA/PIA in Section 2.A.13:

a. **System Security Plan (SSP)** – due within *[insert contract specific timeline]* after contract award. The SSP shall be compliant with the NIST SP 800-18 , *Guide for Developing Security Plans for Federal Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf), the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems* (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf), and NIST SP 800-53 (latest revision) (http://csrc.nist.gov/publications/), *Security and Privacy Controls for Federal Information Systems and Organizations* and other applicable NIST guidance. The SSP shall be consistent with and further detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the

system environment and security requirements to protect the information system as well as describe the 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 update the SSP at least ***annually*** thereafter.

b. **Security Assessment Plan/Report (SAP/SAR)** – due within *[insert contract specific timeline]* after contract award. The security assessment shall be conducted by an independent assessor and be consistent with NIST SP 800-53A, NIST SP 800-30 (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf), latest revisions, and any additions or augmentations described in the HHS IS2P. The assessor will document the assessment results in the SAR. The Contractor shall update the SAR at least ***annually*** thereafter.

c. **Plan of Actions and Milestones (POA&M)** – due within *[insert contract specific timeline]* after contract award. The Contractor is responsible for mitigating all security risks found during continuous monitoring and security reviews. All high-risk vulnerabilities must be mitigated within *2 days* and all moderate risk vulnerabilities must be mitigated within *7 days* from the date vulnerabilities are formally identified. *DCAS* will determine the risk rating of vulnerabilities.

Identified risks between required security control baselines, continuous monitoring controls, and the Contractor's implementation, as documented in the SAR, shall be tracked by the Contractor for mitigation in the POA&M documentation. Depending on the severity of the risks, *DCAS* may require them to be remediated before an Authorization is issued, as applicable.

d. **Contingency Plan and Contingency Plan Test** – due within *[insert contract specific timeline]* after contract award. The Contractor shall develop a Contingency Plan in accordance with NIST SP 800-34, latest revision (http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf), HHSAR, and HHS IS2P. Upon acceptance by the System Owner, the Contractor shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results. The Contractor shall update and test the Contingency Plan at least ***annually*** thereafter.

e. **Security Review** – The Contractor shall ensure an independent security control assessment and review of all applicable security requirements are conducted at least annually and provide to the COR and/or Contracting Officer verification that the system ATO remains valid. Evidence of a valid system security authorization includes written results of (A) annual testing of the system contingency plan and (B) the performance of a security control assessment. Upon the ATO award, Contractor-operated systems that input, store, process, output, and/or transmit shall meet or exceed the continuous monitoring requirements identified below.

f. **E-Authentication Questionnaire** – The contractor shall ensure that an E-Authentication Threshold Analysis (ETA) is completed to determine if a full E-Authentication Risk Assessment (ERA) is necessary. System documentation developed for a system using ETA/ERA methods should follow OMB 04-04 (https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf) and NIST SP 800-63, Rev. 2 *Electronic Authentication Guidelines* (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf).

2. Government Access for IT Inspection. The Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of IT inspection (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.

   a. The contractor, and any subcontractor at any tier handling or accessing protected information, shall 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/subcontractor local time, to access 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.

b. The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the 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, SQL injection vulnerabilities, and any other known vulnerabilities.

c. The contractor, and any subcontractor at any tier handling or accessing protected information, shall fully cooperate with all audits, inspections, investigations, or other reviews. 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.

d. The contractor and any relevant subcontractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

e. The contractor's (and any subcontractor's) cooperation with inspections, audits, investigations, and reviews shall be provided at no additional cost to the Government.

i. These requirements are in addition to the inspection clause in the contract.

ii. These requirements shall continue at all times during contract performance, and even after the contract performance period has ended, until the Contracting Officer consents to closure activities on the contract (including any disposition of data).

f. The contractor shall include sufficient representations in its proposal to demonstrate that it and its relevant subcontractors consent to and shall meet these requirements.

3.A.3. **Information Security Continuous Monitoring**. All Contractor/subcontractor-owned/operated systems that input, store, process, output, and/or transmit HHS information shall meet or exceed the information security continuous monitoring (ISCM) requirements identified in FISMA. The Contractor (and/or any subcontractor) shall also store ***monthly*** ISMC data at its location for a period not less than ***one year*** from the date the data is created. The ***monthly*** ISCM data shall be encrypted in accordance with FIPS 140-2 *Security Requirements for Cryptographic Modules* (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform ISCM and IT security scanning of Contractor (and/or any subcontractor) systems and environment from Government tools and infrastructure.

1. Asset Management. The contractor (and/or any subcontractor) shall use any available Security

Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans to provide an inventory of all information technology (IT) assets for both hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing government owned information/data. It is anticipated that this inventory information will be required to be produced at least 30 days. The contractor (and/or any subcontractor) shall be capable of providing detailed IT asset inventory information, to include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor (and/or any subcontractor) shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

2. Configuration Management. The contractor (and/or any subcontractor) shall use available SCAP-compliant automated tools, per NIST IR 7511 (http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7511r4.pdf), for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that are processing government owned information/data. Compliance will be measured using IT asset and system security configuration guidance provided by the government, for all IT assets. The SCAP-compliant automated tools will compare the installed configuration to the government specific security configuration guidance; contractor may reflect the most restrictive security configuration mode consistent with operational requirements. It is anticipated that this IT asset security configuration information will be required to be produced at least monthly. The contractor shall work towards ultimately maintaining a capability to provide security configuration compliance information for 100% of IT assets using SCAP-compliant automated tools.
3. Vulnerability Management. The contractor (and/or any subcontractor) shall use SCAP-compliant automated tools for authenticated scans to detect any security vulnerabilities in all information technology (IT) assets, (computers, servers, routers, Web applications, databases, operating systems, etc.) that are processing government owned information/data. It is anticipated that this IT asset security vulnerability information will be required to be produced at least ***monthly***. Contractors (and/or any subcontractors) shall actively manage system vulnerabilities using automated tools and technologies where practicable. Automated tools shall be complaint with NIST specified SCAP standards for vulnerability identification and management. Additionally, contractors without in-place automated SCAP-compliant vulnerability management tools and technologies, are required to provide the number of systems (expressed in a percentage) that vulnerability information can be obtained for along with plans for procuring and implementing automated tools that comply with HHS requirements. The contractor (and/or any subcontractor) shall work towards ultimately maintaining a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools.
4. Data Protection. Current Federal government security guidance requires that sensitive government information that is stored on laptops and other portable computing devices shall be encrypted using Federal Information Processing Standard (FIPS)-140-2 validated encryption. The contractor shall provide the percentage of portable IT assets that are equipped with FIPS 140-2 validated encryption, to encrypt all sensitive government information, via a report on a ***quarterly*** basis. Additionally, ensure that all privacy controls are implemented and working as intended.
5. Remote Access. Current Federal government security guidance requires that two-factor authentication be implemented when remotely accessing sensitive government owned information/data on IT systems (both government owned and contractor owned systems). Additional Federal government security guidance when remotely accessing government owned information/data include the following: connections shall utilize FIPS-140-2 validated encryption; connections shall be capable of assessing and correcting system configurations upon connection; connections shall be capable of scanning for viruses and malware upon connection; connections shall prohibit split tunneling; and connections shall require timeout after ***15 minutes*** of inactivity. Each quarter, the contractor shall provide the following information about the contractor's remote access solutions to government owned sensitive information/data: percentage of current connections that allow connection using only a password; percentage of connections that require the use of a government provided personal identity verification (PIV) card as part of a two-factor solution; percentage of connections that require the use of other two- factor authentication solutions; percentage of connections that utilize FIPS-140-2 encryption;

percentage of connections that assess and correct system configurations upon connection; percentage of connections that scan for viruses and malware upon connection; percentage of connections that prohibit split tunneling; and percentage of connections that require timeout after ***15 minutes*** of inactivity.

6. Continuous Vulnerability Remediation. The contractor (and/or any subcontractor) shall install critical security patches or take other security remediation action to resolve weaknesses in systems processing government owned information/data. The contractor shall report status and when the directed action has been completed.
7. Secure Coding. The contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards (https://buildsecurityin.us-cert.gov/resources/secure-coding-sites) and the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide), that will limit system software vulnerability exploits.
8. End of Life Compliance. The contractor must use Commercial Off The Shelf (COTS) software that is supported by the manufacturer. In addition, the COTS software needs to be within one major version of the current version; deviation from this requirement will only be allowed by the HHS waiver process (approved by HHS CISO). The contractor shall provide a quarterly report of all COTS software components and their compliance to this requirement.

3.A.4. Standard for Security Configurations. The Contractor (and/or any subcontractor) shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS (http://intranet.hhs.gov/it/cybersecurity/enterprise_security/config_mgmt/).

3.A.5. Desktop and/or Laptop Computers Required for Use by the Contractor. The Contractor (and/or any subcontractor) shall ensure that IT equipment that is used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations, as follows:

1. The Contractor (and/or any subcontractor) shall configure its computers that contain HHS data in accordance with the latest applicable United States Government Configuration Baseline (USGCB) (http://usgcb.nist.gov/) and/or other approved HHS IT security configurations.
2. The Contractor (and/or any subcontractor) shall ensure that its computers have and maintain the latest operating system patch release and anti-virus software definitions.
3. The Contractor (and/or any subcontractor) shall ensure hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above.
4. The Contractor (and/or any subcontractor) shall validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching.
5. The Contractor (and/or any subcontractor) shall use automated means to ensure that its computers remain in compliance with the above configuration requirements by:
   a. Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; or where such outside scanning is not practicable.

   b. Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems on at least a monthly basis and report the results of these scans to the COR and/or Contracting Officer, Project Officer, and any other applicable designated POC.

3.A.6. Other Computing Devices Required for Use by the Contractor. These computing devices include ancillary and peripheral IT devices as well as other computing servers, but not desktop and/or laptop computers).

1. The Contractor (and/or any subcontractor) shall ensure that information technology (IT) that is used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations, as follows:

a. The Contractor (and/or any subcontractor) shall configure all ancillary and peripheral IT devices and computers that are not desktops or laptops (e.g. servers, routers, mobile devices, etc.) that store and/or transport HHS data, in accordance with the applicable HHS and/or DCAS requirements and ensure that they have and maintain the latest operating system patch level and anti-virus software level, when applicable.

b. The Contractor (and/or any subcontractor) shall ensure that all ancillary and peripheral IT devices and other computing devices, as applicable, have and maintain the latest operating system patch release and anti-virus software definitions.

c. The Contractor (and/or any subcontractor) shall ensure hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above.

d. The Contractor (and/or any subcontractor) shall validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching.

e. The Contractor (and/or any subcontractor) shall use automated means to ensure that its computers remain in compliance with the above configuration requirements by:

i. Configuring systems to allow for periodic HHS vulnerability and security configuration assessment scanning; or where such outside scanning is not practicable.

ii. Using Security Content Automation Protocol (SCAP)-validated tools, per NIST IR 7511 "SCAP Version 1.2 Validation Program Test Requirements, Rev. 4" (http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7511r4.pdf), to scan its systems on at least a *[insert DCAS specific timeframe]* and report the results of these scans to the COR and/or Contracting Officer.

4.A. Hardware Acquisitions

4.A.1. The Contractor (and/or any subcontractor) shall include Federal Information Processing Standard (FIPS) 201-compliant (https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage) smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops; in compliance with FAR Part 12 – Acquisitions of Commercial Items (https://www.acquisition.gov/far/html/FARTOCP12.html) and FAR Subpart 4.13- Personal Identity Verification (https://www.acquisition.gov/sites/default/files/current/far/html/Subpart 4_13.html).

*(**NOTE**: COs/CORs must consult the OMB M-16-02, "Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops" https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf) before procuring Desktop and laptop equipment.)*

4.A.2**. Mobile Devices**. The contractor shall ensure that NIST 800-124, Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) is followed when using mobile devices that process or store HHS data.

4.B. Information Technology Application Design or Support

The Contractor (and/or any subcontractor) shall ensure IT applications designed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges per the HHSAR Subpart 352.239-70--Standard for Security Configurations.

Acronyms

ASA	Assistant Secretary for Administration
ASFR	Office of the Assistant Secretary for Financial Resources
BI	Background Investigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officers Representative
CSIRC	Computer Security Incident Response Center
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
DA	Division of Acquisition
DCAS	Division of Compensation and Anlayisis
E-Auth	Electronic Authentication
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GB	GigaByte
HHS	Department of Health and Human Services
HHSAR	Health and Human Services Acquisition Regulations
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
IS2P	Information Systems Security and Privacy Policy
ISSO	Information Systems Security Officer
IT	Information Technology
M	Memorandum
MBI	Minimum Background Investigation
NACI	National Agency Check and Inquiry Investigation
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NIOSH	National Institute Occupational Safety and Health
OCIO	Office of the Chief Information Officer
OGAPA	Office of Grants and Acquisition Policy and Accountability
OMB	Office of Management and Budget
OpDiv	Operating Division
OSSI	Office of Security and Strategic Information
PII	Personally Identifiable Information
PIV	Personal Identification Verification
PL	Public Law
PM	Program Manager
RBT	Role Based Training
RFP	Request for Proposal
RoB	Rules of Behavior
SCAP	Security Content Automation Protocol

SORN	System of Record Notice
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan
STAFFDIV	Staff Division
USGCB	United States Government Configuration Baseline
USC	United States Code