SSA INFORMATION SECURITY AND GENERAL PRIVACY REQUIREMENTS

1. Definitions. The following terms are defined for the purposes of these requirements.

"**Authorization to Operate (ATO)"** – The official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.

"**Breach**" means the loss of control, compromise, unauthorized disclosures, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses confidential information; or (2) an authorized user accesses or potentially accesses confidential information for an other than authorized purpose. This includes a breach in any medium or form, including paper, oral, and electronic. A breach is not limited to an occurrence where a person other than an authorized user potentially accesses confidential information by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include confidential information and portable electronic storage media that store confidential information, the inadvertent disclosure of confidential information on a public website, or an oral disclosure of confidential information to a person who is not authorized to receive that information. It may also include an authorized user accessing confidential information for other than an authorized purpose. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves confidential information, as is often the case with a lost or stolen laptop or electronic storage device.

"**Confidential information**" means information or data, or copies or extracts of information or data, that is: (1) provided by the Social Security Administration (SSA) to the contractor for, or otherwise obtained by the contractor in, performing work under this contract; and (2) of a personal nature about an individual, such as name, home address, and social security number; proprietary information or data submitted by or pertaining to an institution or organization, such as employee pay scales and indirect cost rates; sensitive information; controlled unclassified information; Federal Tax Information; or information designated by SSA as confidential for other reasons. Confidential information includes all personally identifiable information (PII) provided by SSA to or collected or acquired by the contractor as a result of this contract. Aggregations and tabulations of such PII, as well as de-identified

individual-level data, shall also be treated as confidential information, unless SSA has provided written approval for public dissemination.

"**Controlled Unclassified Information (CUI)**" means non-classified information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

"Federal information" means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

"Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. An information system that does not meet such criteria is a **"nonfederal information system"**.

"**Federal Tax Information (FTI)"** FTI is information that SSA obtains from the Internal Revenue Service (IRS) or on behalf of IRS. FTI is also referred to as "tax return information" or "return information." FTI is governed by the Internal Revenue Code (IRC). The IRC defines "return information to include "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over-assessments, or tax payments. 26 U.S.C. § 6103(b). FTI is categorized as Sensitive But Unclassified information and may contain personally identifiable information (PII).

"Federal Websites and Digital Services". Federal agency public websites and digital services are defined as online information resources or services maintained in whole or in part by the departments and agencies in the Executive Branch of the U.S. Federal Government that are operated by an agency, Contractor, or other organization on behalf of the agency.

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

"Nonfederal information system". An information system that does not meet the criteria of a federal information system.

"**Personally Identifiable Information (PII)**" Information that can be used to distinguish or trace an individual 's identity, either alone or when combined with other information that is linked or linkable to a specific individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, names, Social Security numbers (SSNs) financial account numbers, birth dates, and biometrics identifiers (e.g. fingerprints and facial images). PII only includes information that is made or becomes available to the Contractor as a result of performing under this contract or provided by SSA.

"Plan of Action and Milestone (POA&M)" – is a corrective action plan to track and resolve identified system security weakness.
"Secure area" or **"Secure duty station"** means, for the purpose of this clause, either of the following, unless the agency expressly states otherwise on a case-by-case basis: (1) a Contractor employee's official place of work that is in the Contractor's established business office in a commercial setting, or (2) a location within the agency or other Federal- or State-controlled premises, or (3) a remote work environment (when remote work is authorized by the agency. A person's private home, even if it is used regularly as a "home office" (including that of a Contractor management official), shall not be considered a secure area or duty station.
"**Sensitive Information**" means information or data of which the loss, misuse, unauthorized access to, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled to under 5 U.S.C. § 552a (the Privacy Act), but which no Executive Order or Act of Congress has specifically authorized to be kept secret in the interest of national defense or foreign policy.
"**Suspected breach**" An unconfirmed breach. See the definition of breach for more information.

2. Information Security and Privacy Governance.

The Contractor shall comply with the laws, regulations, directives, policies, standards, and guidelines listed in *Appendix C* - *Attachment A*, as well as any applicable amendments published after the effective date of the contract. In all cases where this contract references federal guidance (including but not limited to SSA policies, OMB guidance and memorandums, and NIST guidance and publications), the Contractor shall comply with the most recently published, final version of that guidance. If such guidance is rescinded completely or there is a question about which version the Contractor must comply with, the Contractor shall seek clarification from the COR.

The Contractor shall confirm and attest compliance with SSA's information security and privacy requirements in this contract prior to award and shall maintain compliance with each requirement throughout the duration of the contract, through contract closure or termination.

3. Subcontractors.

The Contractor shall include all privacy and security requirements in this contract in all resulting subcontracts whenever there is any indication that the subcontractor(s) and their

personnel, or successor subcontractor(s) and their personnel, will or may perform work that would be subject to such requirements if performed by the Contractor. When a subcontract is awarded, all references to "Contractor" in all privacy and security requirements in this contract apply to subcontractor(s).

The Contractor shall retain operational configuration and control of any systems used to process and store federal information, including any systems used in remote work environments (when remote work is authorized by the agency). The Contractor shall not subcontract the operational configuration and control of any system used to process or store federal information.

Note: The subcontractor is required to notify the prime Contractor in instances where the language states the contractor shall notify the agency or COR.

4. Indemnification.

The Contractor shall:

a. Indemnify the agency and its officers, agents, and employees acting for the agency against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into federal information. The Contractor agrees to waive all defenses that may be asserted for its benefit, including (without limitation) the Contractor's Defense.

b. Indemnify the agency and its officers, agents, and employees acting for the agency against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of
    i. The Contractor's unauthorized disclosure of trade secrets, copyrights, contractor bid or proposal information, source selection information, classified information, material marked "Controlled Unclassified Information", information subject to a right of privacy or publicity, personally identifiable information or any record as defined in 5 U.S.C. § 552a; or

    ii. The Contractor's unauthorized introduction of any libelous or other unlawful matter into federal information. The contractor agrees to waive all defenses that may be asserted for its benefit, including without limitation the agency

Contractors Defense.

c. In the event of any claim or suit against the agency on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the agency, when requested by the CO, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Contractor; provided, however, that an equitable adjustment shall be made under this clause, and the contract modified in writing accordingly, if the claim or suit is withdrawn, settled, or adjudicated in favor of the agency, and the basis for the claim or suit, regardless of outcome, was not due to any act or omission of the Contractor.

d. The provisions of this paragraph do not apply unless the agency provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the agency and incorporated in data to which this clause applies. Further, this indemnity shall not apply to:
    i. Disclosure or inclusion of data or information upon specific written instructions of the CO directing the disclosure or inclusion of such information or data;
    ii. Third-party claim that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

5. Safeguarding Federal Information and Information Systems.

The Contractor shall:

a. Protect federal information and information systems to ensure:
    i. *Confidentiality*, which means preserving authorized restrictions on access and disclosure, based on the information security terms found in this contract, including means for protecting personal privacy and proprietary information;

ii. *Integrity*, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and

iii. *Availability*, which means ensuring timely and reliable access to and use of information.

b. Provide security for any information systems, and information contained therein, connected to an SSA network, or operated by the Contractor on behalf of SSA regardless of location. In addition, if the Contractor discovers new or unanticipated threats or hazards to such information systems, and information contained therein, or if existing safeguards to protect such systems and information have ceased to function, the Contractor shall immediately, within one (1) hour, bring the situation to the attention of the COR.
c. Adopt and implement the policies, procedures, controls, and standards, as provided by the COR, 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.
d. Comply with all applicable Privacy Act requirements and FAR and Agency Specific clauses included and referenced in this contract.

6. Information Security Categorization.

The risk level for each security objective (confidentiality, integrity, availability) and the overall risk level, which is the highest watermark of the three security objectives of the information or information system, are the following:

Confidentiality:	[ ] Low	[ ] Moderate	[ ] High
Integrity:	[ ] Low	[ ] Moderate	[ ] High
Availability:	[ ] Low	[ ] Moderate	[ ] High
Overall Risk Level:	[ ] Low	[ ] Moderate	[ ] High

Note: This information security categorization reflects information provided by the Chief Information Security Officer, or other security representative, in accordance with Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60,

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C.

7. Personally Identifiable Information (PII).

Based on information provided by the security or privacy representative, the agency determined that this acquisition includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII:

[ ] No PII [ ] Yes PII

PII Confidentiality Impact Level has been determined to be:

[ ] Low [ ] Moderate [ ] High

8. Minimum Security Baseline.

The Contractor shall ensure that all federal information systems or services it provides shall meet or exceed the minimum-security baseline corresponding to a ***[insert contract-specific impact level]*** -impact system under the latest revision of NIST Special Publication 800-53.

9. Controlled Unclassified Information (CUI).

The Contractor must comply with Executive Order 13556, *Controlled Unclassified Information*, CUI Regulations at (32 CFR, Part 2002); the CUI Registry; and any successor order or regulations when handling CUI. The term "*handling*" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 32 CFR § 2002.4(aa). The Contractor shall safeguard CUI consistent with 32 CFR § 2002.14 and requirements elsewhere in this contract. Misuse of CUI is subject to penalties established in applicable laws, regulations, and Government-wide policies and must be reported to the CO upon discovery. In safeguarding CUI all information shall be:

1. marked appropriately;

2. only disclosed to authorized personnel who have a need for the information in performance of duties under this contract;
3. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, applicable baseline if handled by a Contractor on a federal information system operated on behalf of the agency.

4. protected in accordance with NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, if handled by Contractor on a nonfederal system which has been explicitly approved for use by the CO or COR; and

5. returned to SSA control or disposed of in accordance with the terms of this contract.

The agency determined that this acquisition includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of CUI:

[ ] No CUI [ ] Yes CUI

CUI Category (e.g. PII, FTI [ ]

Note: Additional CUI categories may be identified or created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed as a result of or as part of this contract after the award of this contract and would be subject to this contract. For any questions about CUI, consult with the CO.

10. Protecting CUI on Nonfederal Information Systems.

The Contractor shall not handle federal information with a nonfederal information system unless the CO or COR has explicitly approved such system for use (Authority to Operate (ATO)). The Contractor shall ensure that all nonfederal information systems, which the Contractor is responsible for, that process or store CUI meet or exceed the security controls as specified by NIST SP 800-171.The Contractor shall:

1. Develop policies and procedures to implement security controls and requirements as required by NIST 800-171.

2. Implement continuous monitoring processes to maintain ongoing awareness of nonfederal systems and related security process to ensure compliance with the

security controls as required by NIST 800-171.

3. As requested by the COR, participate in contractor security reviews, provide current documentation describing security controls, coordinate inspections, if the agency requests, and plan for and perform remediation activities to address weaknesses.

4. Ensure that CUI is returned, disposed, or destroyed in accordance with SSA requirements for termination of a contract.

11. Privacy Threshold Analysis (PTA)/Privacy Impact and Risk Assessment (PIRA).

The Contractor shall assist the agency with conducting a Privacy Threshold Analysis (PTA) or Privacy Impact and Risk Assessment (PIRA) for the information system or information handled under this contract as deemed necessary by the agency. The primary purpose of the PTA or PIRA is to determine the need for a Privacy Impact Assessment (PIA) or systems of records notice, or updates to those documents. Assistance from the contractor will consist of providing documentation, such as, but not limited to a Business Process Description, messages on screens, privacy notices, screening tools, and email or text communication.

1. If the agency's PTA/PIRA determination finds that a new or modified PIA is needed, the Contractor shall assist the agency with completing documentation required for a PIRA for the system or information. The contractor shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than ***[insert contract specific timelines]*** days after the documentation or information has been requested by the COR.
2. The Contractor shall assist the COR or designee in reviewing the PIRA at least every [***insert contract-specific timeline***] throughout the system development lifecycle/information lifecycle, or when the agency determines that a review is required based on a major change to the system, when the system processes new information types, or when the system introduces new or increased privacy risks, whichever comes first.

12. Digital Identity Risk Assessment (DIRA)

The Contractor is required to adhere to requirements in the latest version of NIST SP 800-63.

The Contractor shall assist SSA with conducting a Digital Identity Risk Assessment (DIRA) for the information system or information handled under this contract as deemed necessary by SSA. A DIRA is required for all public-facing applications and automated telephone services (digital services). The DIRA determines the required identity proofing, authentication, and federation security levels for digital services. Assistance from the Contractor will consist of meeting with the SSA DIRA team and providing all documentation requested, including copies of all screens and a detailed business process description.

a. If the DIRA determination finds that a DIRA is required, the Contractor shall assist SSA with completing documentation required for a DIRA for they system. The contractor shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than *[insert contract specific timelines]* days after the documentation or information has been requested by the COR.
b. The Contractor shall assist the COR or designee in reviewing the DIRA at least every *[insert contract specific timelines]* throughout the system development lifecycle/information lifecycle, or when the agency determines that a review is required based on a major change to the system, when the system processes new information types, or when the system introduces new or increased digital identity or information security risks, whichever comes first.

RULES OF BEHAVIOR

The Contractor shall comply with SSA's Rules of Behavior for Users as follows:

1. Accountability
    a. Comply with current information security, privacy, and confidentiality practices.
    b. Behave in an ethically, informed, and trustworthy manner.
    c. Be accountable for all transactions issued in connection with their account credentials.
    d. Never share password with anyone.
    e. Have formal authorization from their COR (or other specified management official or representative) before accessing sensitive or critical applications.
    f. Only use provided access as necessary to execute the contract requirements.

2. Integrity
    a. Never intentionally enter unauthorized, inaccurate, or false information.
    b. Never expose critical data or sensitive information to conditions that may compromise the data's integrity.
    c. Review the quality of information as it is collected, or generated to ensure that it is accurate, complete, and up to date.

d. Take appropriate training before using a system.

3. Confidentiality
    a. Disclose information obtained in the performance of their duties only as necessary to execute the contract requirements and as permitted by agency regulations and guidance and federal regulations, guidance and law.
    b. Take precautions to eliminate access or exposure to sensitive information by unauthorized parties or devices.
    c. Log-off or lock workstations when leaving devices unattended.

4. Awareness and Training
    a. Be alert to any indicators of system abuse or misuse.
    b. Complete the mandatory Information Security and Privacy Awareness Training and, if required, Role Based Privacy Training, within agency specified timeframe.
    c. Participate in all required Information Security training and awareness activities as identified by management or required by policy.

5. Sensitive Information
    a. Protect all sensitive information whether officially on duty or not on duty, at an SSA site, another official work location, or an alternate worksite.
    b. Agree to follow all requirements for protecting and handling PII and CUI, including in this contract, FAR and Agency Specific clauses, and any task order issued under this contract.

6. Hardware, Software, and Copyright Protection and Control
    a. Do not disable any SSA security features unless authorized by management.
    b. Use only approved SSA systems resources on SSA equipment. Connecting personally owned hardware, software, and media to SSA systems resources is prohibited.
    c. Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices (PED) against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures.
    d. Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws.
    e. Do not make illegal copies of software.
    f. Under no circumstances shall SSA equipment be used for any activity other than official SSA business conducted under this contract and any task order issued under this contract.
    g. Comply with all SSA policy and procedures regarding the use of e-mail as well as other forms of electronic communications.
    h. Properly safeguard removable media.

7. Alternative Worksite (Non-SSA Controlled Locations)
    a. Follow the security and safety requirements of an alternative worksite requirements defined in the task order.

b. Adhere to all rules of behavior requirements while at the alternative worksite.
c. Do not print any material that contains PII at non-SSA controlled locations unless specifically allowed in the contract.
d. Safeguard and properly dispose of any other sensitive printed material.

8. Public Disclosure
    a. Contractor staff that are required to use social media in an official capacity on behalf of the agency must follow the mandatory guidance outlined in this contract and any task order issued under this contract.
    b. Ensure the appropriate SSA management officials approve SSA information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers.
    c. Never transmit, store, or process sensitive or proprietary SSA information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers.
    d. Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

9. Incident Reporting
    a. Report suspected virus attacks and malicious/unauthorized intrusion or access in accordance with this contract and any task order issued under this contract.
    b. Report suspected violations of the Social Security Act, Privacy Act, and other laws, as well as SSA policies and procedures to the COR.

10. Consequences of Rules Violations

    In those instances where users do not follow the prescribed rules of behavior or violate other agency information security polices, SSA may suspend or remove access to systems or require the return of SSA equipment, any of the above, or other options available under this contract and applicable federal law. SSA may pursue as appropriate other penalties and legal actions. The CO will officially inform the contractor's representative for the contract of the violation.

PHYSICAL LOCATION AND DATA JURISDICTION REQUIREMENTS

1. The Contractor shall be located, and shall ensure that all federal information is accessed, transferred, stored, or processed, only within the sole jurisdiction of the United States (U.S.) (i.e., any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands). All Contractor primary locations, back-up facilities or archiving facilities, sites where antivirus and other security scans are performed, and locations of personnel who provide support to SSA in resolving issues regarding the solution, must be physically located within the sole jurisdiction of the United States (as defined). This includes, but is not limited to, the Contractor's primary headquarters facilities, the physical location of all information systems, and the geographical origin of all software used in the execution of this contract.

2. The Contractor shall provide the CO and COR with the specific address for the physical location of all facilities hosting information systems relevant to the execution of this contract. If requested by the CO or COR, the contractor shall provide physical access to the hosting facility for inspection.

3. At the request of the CO, the Contractor shall provide immediate logical and physical access to all federal information to allow the agency to conduct a review, scan, or a forensic evaluation of any contractor facility where federal information is located. If the federal information is co-located with nonfederal information, the Contractor shall isolate the federal information into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized agency personnel identified by the CO, and without the Contractor's involvement.

4. The Contractor shall notify the CO and COR at least 30 days prior to moving its physical site and within 24 hours when the hosting location of confidential information changes servers or devices. The new location must meet or exceed the security requirements for the current site.

DATA PROTECTION REQUIREMENTS

1. **Inventory**. The Contractor shall maintain a complete inventory of all hardware and software used in the execution of the contract, including model or version numbers. If the Contractor is processing, storing, or transmitting PII/CUI, the Contractor must indicate in the complete inventory which systems process that information. The Contractor shall provide this inventory information to the CO or COR, upon request.

2. **Manufacturer Support**. The Contractor must ensure that all software used in execution of this contract is within one major version of the current version. The Contractor must ensure that all software and hardware used in execution of this contract has manufacturer support. The Contractor must retire or upgrade all software and systems that have reached end-of-life.

3. **Standard for Encryption of electronic information**. The Contractor shall:
   a. **NOT** decrypt information they are unauthorized to view.

   b. Encrypt all confidential information (e.g., PII/CUI, proprietary information) in transit (e.g., email, network connections) and at rest (e.g., servers, storage devices, mobile devices, backup media) with FIPS 140-2 (Level 2) validated encryption solution that provides for origin authentication, data integrity, and signer non-repudiation.

   c. Secure all devices (e.g., desktops, laptops, mobile devices) that store and process confidential information and ensure devices meet any SSA specific encryption standard requirements referenced in this contract. Maintain a complete and current inventory of all devices and portable media, as referenced below, that store or process federal information.

   d. Verify that it validates the encryption solutions in use under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR upon request.

   e. Use the Key Management system on the SSA personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.
4. **Media Transport.** The Contractor shall:
   a. Document activities associated with the transport of federal information stored on digital and non-digital media.

   b. Digital media, containing federal information that is transported outside of controlled areas shall be encrypted using FIPS 140-2 level 2; non- digital media must be secured using the same policies and procedures as paper.

c. Media, containing federal information that is transported outside of controlled areas shall be documented in logs, which the agency may request at any time, that include:

    i. Identifier and description of what was transported

    ii. Date of transportation and destination

    iii. Names of personnel who handled the media during transit outside of controlled areas

    iv. Date the media was returned or destroyed

    v. Name of personnel who received the returned media

    vi. Notes of any damage to the media at arrival.

5. **Boundary Protections.** The Contractor shall ensure that federal information, other than unrestricted information, being transmitted from Federal government entities to external entities is inspected by Trusted Internet Connections (TIC) processes.

6. **Configuration Baselines.** The Contractor must ensure that they deploy and operate all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) and software used to process information on behalf of SSA in accordance with approved security configurations and meet the following minimum requirements:

a. Encrypt equipment and confidential information stored or processed by such equipment in accordance with FIPS 140-2 encryption standards;

b. Configure all hardware and software in accordance with the latest applicable United States Government Configuration Baseline, FAR Subpart 39.101(c), Defense Information Systems Agency Security Technical Implementation Guides, Center for Information Security Benchmarks, or any other minimum security configuration standards as identified by the CO or COR;

c. Maintain the latest operating system patch release and anti-virus software definitions;

d. 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;

e. Automate configuration settings and configuration management in accordance with SSA security policies, including but not limited to:

   i. Configuring its systems to allow for periodic SSA vulnerability and security configuration assessment scanning; and

   ii. Using Security Content Automation Protocol-validated tools with configuration baseline scanning capabilities to certify all products operate correctly with SSA and NIST defined configurations and do not alter these settings. The Contractor must scan its systems on at least a monthly basis and report the results of these scans to the COR.

7. **Federal Websites and Digital Services**. The Contractor must securely configure all new and existing Federal agency public websites and digital services with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain Hypertext Transfer Protocol. For internal-facing websites, the HTTPS is also required.

Contractors tasked with creating, maintenance, or operating SSA public facing websites must comply with all applicable Federal laws, regulations, and policies, in addition to obtain agency approval as directed by the COR. SSA public facing websites are subject to federal and agency specific Internet privacy policies and federal security policies including, but not limited to, OMB M-10-22, M-23-22, and any superseding policies.

8. **Binding Operational Directives.** The Contractor shall comply with all Binding Operational Directives (BOD). (https://cyber.dhs.gov/directives/)

9. **Secure Email Requirements**. The Contractor's corporate or organizational email system is deemed not to be secure. Therefore, the Contractor shall put policies and procedures in place to ensure that its personnel email confidential information using only the following procedures in (a) - (b), below:

a. Sending from an SSA email address. If personnel have been given access to the SSA email system, they may use it to send email messages containing confidential information in the body or in an unencrypted attachment but only to other SSA email addresses (which contain the "name @ssa.gov" format) or to email addresses belonging to an SSA-certified email system. Email directed to any other address(es) may contain confidential information only if the confidential information is entirely

contained in an encrypted attachment. The Contractor shall encrypt confidential information in accordance with OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).

b. Sending from a non-SSA email system. If personnel are using the Contractor's own or any other non-agency email system (e.g., Yahoo!, Gmail), they may send email messages transmitting confidential information only if the confidential information is entirely contained in an encrypted attachment, per OMB Circular A-130; none of the confidential information may be in the body of the email itself or in an unencrypted attachment. When emailing from such systems, this procedure applies when emailing confidential information to any email address, including but not limited to, an SSA email system address. Unless specifically noted otherwise, the Contractor and its employees are expected to conduct business operations under this contract using the Contractor's own email system, i.e., in accordance with the foregoing rules for transmitting confidential information.

Note: SSA may grant written exceptions to compliance with the email requirements above when the Contractor's corporate or organizational email system has been deemed by SSA to be secure.

10. **Data Access and Use Requirements**. The Contractor shall:

a. **NOT** access, use, or disclose confidential information, except as necessary to execute the contract requirements.

b. Only disclose confidential information to authorized Contractor personnel who need the information or equipment in the performance of work under this contract. The Contractor shall ensure they establish appropriate administrative, technical, and physical safeguards to ensure that they properly protect security and confidentiality of such information and equipment.

c. Document all activities associated with the transport of confidential information, including devices and media containing such information, transported outside controlled areas or facilities. This includes the transport of information stored on digital and non-digital media and mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

11. **Non-Disclosure of Information.** If the Contractor receives a request, subpoena, or court order for agency confidential information, the Contractor will promptly provide (within two business days) the CO notice of such request. The Contractor will provide the agency with the information or tools required for the agency to respond to the request, if necessary. The Contractor shall refer the requester to the agency. The Contractor will not provide a

requester any agency confidential information unless authorized by the agency. The Contractor shall not provide testimony in legal proceeding about agency functions or information unless such action is approved by the agency and consistent with 20 C.F.R. Part 403.

12. **Data Retention, Inspection, and Disposal Requirements**. The Contractor shall:
    a. Allow the agency the ability to immediately access, search, locate, collect, preserve, amend, and process SSA confidential information as needed to comply with requirements under the provisions of both the Freedom of Information Act (5 U.S.C. § 552); the Privacy Act (5 U.S.C. § 552a); or other Federal law.

    b. Offer capabilities to support the agency's ad hoc legal requirements for E-Discovery, such as litigation preservation obligations, and other preservation or production orders, including meta-data. The Contractor must allow SSA the ability to immediately access, search, locate, collect, preserve, and process SSA confidential information to comply with E-Discovery obligations.

    c. NOT dispose of any SSA information unless authorized by SSA. The Contractor must document and report within 24 hours to the COR all events of accidental disposal or destruction of SSA information without proper authorization as an incident of data loss.

    d. Provide immediate physical and logical access to allow the agency to conduct an inspection. The program of inspection shall include, but is not limited to, conducting authenticated and unauthenticated operating system/network/database/web application vulnerability scans. SSA personnel, or agents acting on behalf of SSA, may perform automated scans. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol standards and the agency approved them. The agency may request the Contractor's scanning results and, at agency discretion, accept those in lieu of agency performed vulnerability scans.

    e. At the direction of the COR, within *[Specify Number of Days]* days following the agency's final acceptance of the work under this contract or expiration or termination of this contract, whichever occurs first, the Contractor must return all federal information and IT resources acquired during the term of this contract to the COR, including but not limited to SSA information in non-federal systems, media, and backup systems. The Contractor must provide the agency all materials embodying SSA confidential information (in any form, and including, without limitation, all summaries, copies, excerpts, and metadata of SSA confidential information) to SSA,

at no additional cost to SSA. Physical items returned to the agency shall be hand carried or sent by certified mail to the COR.

f. At the direction of the COR, properly sanitize and purge all electronic information obtained in execution of this contract from all Contractor-owned systems including backup systems and media used during contract performance, in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*. The Contractor must provide a certification to the COR that the Contractor properly sanitized, purged, and destroyed electronic and physical records of SSA information obtained in execution of this contract.

13. **Audit Record Retention**. The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to capabilities such as those identified in:

a. DoD STD-5015.2 V3 (ref. b), Electronic Records Management Software Applications Design Criteria Standard,

b. NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail (ref. c),

c. NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud Computing Environments (ref 8).

d. SSA Information Security Policy (ISP): Low impact systems – at least 30 days; Moderate impact systems – at least 90 days; High impact systems – 7 years.

14. **Risk Remediation**. The Contractor shall:

a. Mitigate security risks for which they are responsible, including those identified during Security Assessment and Authorization (SA&A) and continuous monitoring activities. Remediate all vulnerabilities and other risk findings. As required by the NIST SP 800-53, Moderate security controls baseline, the contractor must mitigate high-risk vulnerabilities identified during penetration testing, and monthly vulnerability scans within thirty days from date of discovery. Mitigate moderate-risk vulnerabilities within ninety days from date of discovery.

b. In the event the Contractor cannot mitigate a vulnerability or other risk finding within the prescribed timelines above, work with the COR to add them to the

designated Plan of Action & Milestone Report (POA&M) and mitigate them within the designated timelines.

15. **Security Assessment and Authorization (SA&A)**. The Contractor shall:

a. Assist SSA with obtaining an SSA Authorization to Operate (ATO) or Security Approval for the proposed solution prior to processing, collecting, or transmitting information. All External Service Providers (ESP) that process or store PII are considered a Moderate impact categorization, at minimum. If PII or sensitive data (defined by the COR) is stored or processed by the ESP, then the ESP shall provide a Security Authorization Package (SAP), which must be reviewed and updated annually to establish and maintain authorization or approval to continue the work. The SAP must include a System Security Plan (SSP), Security Assessment Report (SAR), provided annually by a third-party assessment group, and Plan of Action & Milestone Report (POA&M) with severity and timelines for remediation. All security assessments, reports and resulting POA&Ms must be inline and compliance with all applicable NIST and OMB policies and guidance (NIST 800-37, NIST 800-115, OMB M-02-01, etc.) The ESP shall conduct a triennial reassessment of the information system in which the contractor shall assess the validity of all current applicable security controls. Additionally, at least annually, the Contractor shall assess a selected subset of the technical, management, and operational security controls employed within the information system. The SAP must be reviewed and approved by SSA before the SSA transfers data to the ESP. Refer to NIST SP 800-37, as updated, for more information on the Security Authorization Package.

b. SSA's issuance of a signed SSA ATO does not alleviate the Contractor's responsibility to ensure system security and privacy controls are operating effectively on an ongoing basis. The Contractor shall ensure system security and privacy controls are operating effectively on an ongoing basis.

16. **Continuous Monitoring.** The Contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements of the NIST Risk Management Framework, and the agency information systems continuous monitoring strategy.

ACCESS CONTROL REQUIREMENTS

Multifactor Authentication. The Contractor shall ensure that all IT products and services are:

- Interoperable with SSA issued PIV smart cards
- Compliant with (or authenticate using) approved phishing-resistant Multifactor Authentication mechanism(s), leveraging existing Agency security infrastructure.

The provider shall implement an authentication solution that integrates with SSA's Federation Service to facilitate end user single-sign on using OpenID Connect (OIDC) or SAML (Security Assertion Markup Language) 2.0 standards.

INCIDENT RESPONSE

The Contractor shall follow the following requirements in the event of an incident involving confidential information. If the Contractor experiences a breach or incident that involves PII, the Contractor shall also follow any additional requirements specific to PII as set forth in the contract.

1. The Contractor shall provide a list of their personnel, identified by name and role, with system administration, monitoring, and/or security responsibilities that are to receive security alerts, advisories, and directives.

2. The Contractor shall have a formal security breach or incident reporting plan approved by the CO or COR. The approved plan shall outline appropriate roles and responsibilities, as well as the steps that must be taken, in the event of a security breach or incident. The plan shall designate who within the Contractor's organization has responsibility for reporting the breach or incident to the agency. The Contractor must follow incident reporting and breach protocols as specified by the agency.

3. The Contractor must cooperate with SSA internal investigation processes with respect to illegal or inappropriate usage of federal information resources including, but not limited to, those investigations conducted by the SSA Office of Human Resources for administrative investigations and those conducted by SSA's Office of the Inspector General.

4. In the event of a suspected or confirmed security-related incident or breach of confidential information, the Contractor shall:

a. Protect all confidential information to avoid a secondary incident with FIPS 140-2 validated encryption.

Limit disclosures about confidential information involved in a breach or incident to only those SSA and Contractor personnel with a need for the information to respond to and take action to prevent, minimize, or remedy the breach or incident. The Contractor may disclose breach or incident information to Federal, state, or local law enforcement agencies and other third parties with a need for the information; however, information about the specific confidential information involved may only be disclosed to such authorities and third parties as Federal law permits.

NOT, without SSA approval, publicly disclose information about confidential information involved in a breach or incident or SSA's involvement in a breach or incident.

NOT, without SSA approval, notify individuals affected by the confidential information breach or incident. The Contractor's confidential information breach and incident reporting process shall ensure that disclosures are made consistent with these requirements.

5. The Contractor shall report all suspected and confirmed security-related incidents and breaches to the SSA COR or designated alternate as soon as possible and without unreasonable delay, **but no later than one (1) hour after discovery**. The Contractor shall provide complete and accurate information about the details of the security-related incident or breach to assist the SSA COR/alternate, including the following information:

a. Contact information;

A description of the security-related incident or breach (i.e., nature of the incident/breach, scope, number of individuals impacted, type of equipment or media, etc.) including the approximate time and location of the security-related incident or breach;

A description of safeguards used, where applicable (e.g., locked filing cabinet, redacted personal information, password protection, encryption, etc.);

An identification of agency components (organizational divisions or subdivisions) contacted, involved, or affected;

Whether the Contractor has contacted or been contacted by any external organizations (i.e., other agencies, law enforcement, press, etc.); and

Any other pertinent information.

6. The Contractor shall provide full access and cooperate on all activities as determined by the agency to ensure an effective incident and breach response, including providing all requested images, log files, and event information to facilitate rapid resolution of confidential

information incidents. This may involve disconnecting the system processing, storing, or transmitting the confidential information from the Internet or other networks or applying additional security controls. This may also involve physical access to Contractor facilities during a breach or incident investigation.

ADDITIONAL INFORMATION SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED SOLUTIONS

NOTE: When the Contractor's proposed solution involves or may involve the use of cloud technology, the Contractor must also comply with all of the following information security and privacy requirements.

1. **FEDRAMP Authorization Requirements**. The Contractor shall comply with FedRAMP SA&A requirements and ensure the information systems and services under this contract have a valid FedRAMP compliant (approved) Authority to Operate (ATO) in accordance with FIPS Publication 199 defined security categorization at the time of contract. If the cloud service product is not listed in the FedRAMP Marketplace (https://marketplace.fedramp.gov/#/products) with a "FedRAMP Authorized" status, the Contractor shall submit a plan to obtain a FedRAMP approved ATO (60) days prior to contract award.

2. **Compliance.** In the event the Cloud Service Provider (CSP) fails to meet both SSA and FedRAMP security and privacy requirements or there is an incident involving confidential information, SSA may suspend or revoke an existing agency ATO (either in part or in whole) and cease operations. If SSA suspends or revokes an agency ATO in accordance with this provision, the CO or COR may direct the CSP to take additional security measures to secure confidential information. These measures may include restricting access to confidential information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the confidential information from the Internet or other networks or applying additional security controls.

3. SSA Authorization Requirements. The Contractor shall:
    a. In addition to the FedRAMP compliant ATO, upon SSA's request, complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service. The SSA authorizing official must approve the agency ATO prior to implementation of the system or acquisition of the service.

b. 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, SSA may require remediation at the Contractor's expense, before SSA issues an ATO.

4. **Physical Access Records.** The Contractor shall record all physical access to the cloud storage facilities and all logical access to the federal information as specified in the contract. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the CO or designee in accordance with the contract or upon request to comply with federal authorities.

5. **Availability.** The Contractor shall inform the COR of any interruption in the availability of the cloud service as required by the service level agreement. Whenever there is an interruption in service, the Contractor shall inform the COR of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor must provide regular updates, at intervals specified by the COR, to the COR on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.

6. **Continued Compatibility.** The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the agency's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing notification, **within 1 hour of discovery**, to the COR and shall be responsible for working with the agency to identify appropriate remedies and if applicable, work with the agency to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7. **Service Level Agreement (SLA).** The Contractor shall understand any applicable terms of the service agreements that define the legal relationships between cloud customers and cloud providers and shall work with SSA to develop and maintain a Service Level Agreement.

8. **Notification Banners.** The Contractor shall display The Standard Mandatory Notice and Consent Banner at log on to all information systems. Choose either banner "a" or "b" based on the character limitations imposed by the system. The formatting of these documents, to

include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."

a. Banner for desktops, laptops, and other devices accommodating banners of 1300 characters.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

For devices with severe character limitations:

I've read & consent to terms in IS user agreem't.

9. **Facility Inspections.** The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the agency conduct a security audit based on the agency's criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the COR within 20 days of

the Contractor's receipt of the audit results. In addition, the agency reserves the right to inspect the facility to conduct its own audit or investigation.

10. **Cloud Security Governance**. The Contractor shall:

a. Ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act of 2002 (44 U.S.C. § 3551, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283)), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide the CO with any documentation it requires for its reporting requirements within 10 days of a request.

Make the environment accessible for an agency security team to evaluate the environment prior to the placement of any federal information in the environment and allow for periodic security reviews of the environment during the performance of this contract. The Contractor shall also make appropriate personnel available for interviews and provide all necessary documentation during these reviews.

11. **Maintenance.** The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to proactively prevent the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the Contractor's PVM systems and programs apply standardized configurations with automated continuous monitoring to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving the agency are compatible with existing systems and architecture of the agency.

12. **Continuous Monitoring.** The Contractor shall provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the COR. In addition, the agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements. If requested, the Contractor will provide the report to the agency within 10 business days.

13. **Penetration Testing.** The SSA reserves the right to perform penetration testing on Contractor's systems, facilities, or cloud services used by the Contractor to deliver services to the SSA. If the agency exercises this right, the Contractor shall allow agency employees (or designated third parties) to conduct security assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning, network device scanning (to include routers, switches, and firewall), Intrusion Detection System/Intrusion Prevention System, databases, and other applicable systems (including general support structure that support the processing, transportation, storage, or security of SSA confidential information for vulnerabilities).

14. **Risk Remediation.** In the event the Contractor cannot mitigate a vulnerability or other risk finding within the prescribed timelines above, and upon agreement with the CO they shall be added by the Contractor to the designated POA&M and mitigated within the agreed upon timelines. SSA will determine the risk rating of vulnerabilities using FedRAMP baselines.