SOCIAL SECURITY ADMINISTRATION
STRENGTHENING PROTECTIONS FOR SOCIAL SECURITY BENEFICIARIES ACT 2018 (SPSSBA)

PROTECTION AND ADVOCACY SYSTEMS (P&A)
AWARD TERMS & CONDITIONS
EFFECTIVE AUGUST 1, 2026

INTRODUCTION, APPLICABILITY, DEFINITIONS, ABOUT THE DOCUMENT, ORDER OF PREFERENCE, AND ROLES AND RESPONSIBILITIES

Introduction. The recipient must comply with the terms and conditions outlined below. These terms and conditions are in addition to the assurances and certifications made as part of the award and terms, conditions, and restrictions reflected on the official award document. Failure to comply with the terms and conditions outlined below and those directly reflected on the official award document may result in enforcement actions as outlined in 2 C.F.R. 200.339 and 200.340.

Note: Correspondence and Maintenance of Official Grant Files:

Your official grant file is maintained in www.GrantSolutions.gov. This system houses copies of all applications, awards, and program and financial reports. Please upload important correspondence as a grant note in GrantSolutions. This includes updated resumes for key personnel, notices of staff changes or anything else pertinent to the management of your program. Should you find it necessary to email your Program of Grants Officer, please include your Grant Award Number (Grant No. SPS23000XXX) in the subject line of your emails.

Applicability. These terms and conditions apply to the Protection and Advocacy Systems (P&A) for the SPSSBA grant program administered by the Social Security Administration (SSA). This grant agreement authorizes the P&A rights to operate an SPSSB project to:

- Conduct assigned representative payee reviews (reviews) and educational visits (visits)

The purpose of the review is to verify that the representative payee is using the benefits properly on behalf of the beneficiary and is carrying out the representative payee responsibilities and duties correctly. The purpose of educational visits is to ensure that payees fully understand their duties and responsibilities and are on the right track with respect to recordkeeping, use of benefits, and reporting.

The applicable sections of the Social Security Act concerning monitoring are: Soc. Sec. Act, 205(j)(3)(A), 1631(a)(2)(C) and 205(j)(6), 1631(a)(2)(G)(i)

About the Document. The document incorporates

- The entire Uniform Guidance (UG), 2 C.F.R. Part 200 by reference;
- The SPSSBA Business Process Document by reference;
- Attachment A – SSA Information Security and General Privacy Requirements (AUG 2026)
- Attachment A.2.A – 2352.224-2A Protecting and Reporting the Loss of Personally Identifiable Information (MAY 2026);

- Attachment A.2.B - 2352.224-2B Worksheet for Reporting a Loss or a Suspected Loss of Personally Identifiable Information (PII) (May 2026);
- Attachment A.2.C - 2352.224-1 Protection of Confidential Information (DEC 2024)
- Attachment B - Security and Suitability Requirements (May 2026);
- Attachment C - Data Protection, Privacy, and Security Requirements;
- Attachment D - Government Property - Grants (SEP 2021);
- Attachment E - Designation of Property Administrator/Listing of Government Property (JUL 2026) - Grants;
- Attachment F - Instructions for Secure Disposal of Confidential Information;
- Attachment G - Guidance and Instructions for Telework;
- Attachment H - Privacy, Disclosure, and Security Authorities (AUG 2024);
- Attachment I - Notice of Specific Terms and Conditions for Risk Tiered Awards (2026)

Precedence. In the event of inconsistencies between provisions of the award, the P&A must promptly contact the Grants Management Officer for clarification. See Federal Awarding Agency Contacts.

Definitions. The following definitions apply to these requirements and the terms of this award. Refer to Attachment A – SSA Information Security and General Privacy Requirements for additional defined terms.

Business Process Document (BPD) means SSA documents furnished to the P&A and National Association Grantee (NAG) describing the processes for conducting reviews and visits for purposes of the SPSSBA grant. These documents include but are not limited to the P&A BPD and NAG BPD. SSA may revise the BPD at any time. The recipient must comply with the revised BPD after the effective date of the SSA action that leads to the revision. Revised processes described in the BPD do not apply to the grantees' activities carried out prior to the effective date of the revision. SSA will inform the recipient of all revisions to the BPD, and the recipient will inform all subrecipients.

SSA Guidance means advice or information issued by SSA to the NAG or P&A that is directed at resolving a problem or situation or clarifying or amending policy, processes, or procedures. Some examples of SSA guidance include emergency instructions, email correspondence, and JIRA software communications. The NAG and P&As must comply with SSA guidance regardless of the means of issuance.

"Award", "grant", "grant award" all mean the award made under SPSSBA to which these terms and conditions apply.

"Recipient", "grantee, "awardee" all mean P&A or National Association entity receiving the award made under SPSSBA.

"Subaward" means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It

does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract. These terms and conditions shall also apply to any subaward.

"Subrecipient", "subgrantee", "subawardee" all mean an entity, usually but not limited to recipients, that receives a subaward from a pass-through entity to carry out part of a Federal award; but does not include an individual that is a beneficiary of such award. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

Due to the nature of the SPSSBA project, subawards may only be granted to subrecipients that are other P&A systems, and the work may only be conducted by P&A personnel that have received appropriate training and a favorable suitability determination.

Roles and Responsibilities. In addition to the roles and responsibilities in the BPD, the following apply as appropriate:

A. Social Security Administration
   (i) Manage and oversee the Representative Payee Monitoring Program.
   (ii) Manage and revise the BPD.
   (iii) Manage all aspects of grants to the P&A and NAG.
   (iv) Prepare and develop review and visit information.
   (v) Furnish a method for receiving questions from the NAG.
   (vi) Approve correctly submitted P&A corrective action plans and Final Report Packages from P&A grantees as defined in the BPD.
   (vii) Oversee quality assurance of P&A and NAG work products.
   (viii) Review and approve all P&A public-facing and publicly distributed materials.
   (ix) Furnish and maintain tools, software, and applications to: manage the review and visit cases, share information, retain documents, facilitate submission of deliverables, and track progress.

B. National Association Grantee
   (i) Provide training, administrative support, technical assistance, and other support for the review and visit program to the state P&As.
   (ii) Coordinate case information with SSA to disseminate to the P&As to support the SPSSB mission and completion of assignments.
   (iii) Establish a training plan to equip the P&A grantees to conduct the required reviews and visits.
   (iv) Establish a process for performing a quality review prior to submitting the final review and visit packages to SSA.
   (v) Submit final review and visit packages to SSA.
   (vi) Ensure compliance with the BPD. Report areas of non-compliance to SSA.
   (vii) Review P&A informational materials (brochures, handouts, forms, articles, guides, instructions, website materials, PowerPoint presentations, etc.) to ensure information complies with the BPD and SSA guidance.

C. Protection and Advocacy System

(i) Conduct representative payee reviews and educational visits in accordance with the terms of this award and the BPD.

In performance under this award, the P&A shall perform the following responsibilities:

1. Representative payee site reviews and educational visits

a. Conduct the following types of reviews and visits in accordance with the BPD and SSA guidance:

Periodic - Reviews identified by SSA as requiring a cyclical review for the following payees: organizational payees serving 50 or more beneficiaries (selected every four years); individual payees serving 15 or more beneficiaries (selected every four years); fee-for-service payees (selected every three years); state onsite (mental institution) reviews (selected every three years).

Predictive Model - Reviews selected by SSA based on case characteristics that indicate a higher likelihood of potential misuse for the following payees: Organizational payees serving 49 or fewer beneficiaries; Individual payees serving 14 or fewer beneficiaries

Quick Response Checks - Reviews conducted in response to concerns about the performance or suitability of a payee.

P&A Initiated – Reviews selected based on a P&A's recommendation that a review is warranted. P&A initiated reviews must be approved by SSA.

Educational Visits – Initial onsite six-month assessments for fee-for service payees or visits conducted anytime SSA determines it is needed for any type of payee. Note: The results of an educational visit may trigger SSA to initiate another type of review.

b. Document reviews and educational visits and develop corrective action plans.

2. Training, Technical Assistance, and Quality Assurance

a. Ensure staff are trained on the BPD and award requirements including any changes or updates that may occur throughout the grant performance period.

b. Receive the NAG's written approval for all instructional material (brochures, handouts, forms, articles, guides, instructions, website materials, PowerPoint presentations, etc.) prior to distributing or presenting to P&A personnel. Ensure instructional content is in accordance with the guidance found in the BPD and SSA guidance.

- P&As must submit materials to the NAG for review and approval. The NAG will ensure materials are presented in compliance with the BPD and SSA guidance. SSA reserves the right to revoke any prior approvals by the NAG at any time.
- P&As should cite their sources and references for training materials (e.g., BPD page XX, section YY, or SSA.gov, etc.)

c. Review case work to ensure compliance with the BPD and SSA guidance. If recurring errors are found, develop training and quality improvement plans for staff.

d. Promptly notify the NAG of any technical assistance and/or training needs.

e. Ensure work products with errors are corrected in a timely manner as guided by the NAG or SSA.

f. Upon request from the NAG or SSA, develop and submit a plan to improve quality of the reviews.

g. Upon request, submit all training plans, records, and materials to SSA.

3. Program Management, Communication, and Staffing

a. Upon request from the NAG or SSA, participate in conferences, meetings, trainings, and calls for the purpose of managing the representative payee program or grants.

b. Cooperate with the NAG and SSA to resolve issues that arise in the daily operations of the program.

c. Maintain open, timely communication with designated NAG and SSA executives and staff to ensure effective support for all site reviews and educational visits.

d. Monitor workloads to ensure the quality of the reviews, including timeliness and accuracy.

e. Ensure corrective action plans and final report packages are complete and accurate prior to submission to the NAG.

f. Ensure timely processing of payee reviews as indicated in the BPD.

g. Maintain sufficient staffing to achieve program objectives.

h. Promptly notify SSA of staffing changes.

i. Ensure all staff with program management and/or oversight responsibilities (including executive and support staff) are suitable and have received a favorable suitability determination issued by SSA. See Attachment B – Security and Suitability Requirements. P&A must maintain at least two individuals who meet SSA's Security and Suitability Requirements at all times.

4. Other Responsibilities

a. Utilize the Representative Payee Monitoring Tool (RPMT) and other tools, software, and applications as directed by SSA, to manage the payee review cases, information sharing, document retention, submission of deliverables, reporting, and tracking progress. Ensure all activity pertaining to the data collection of the representative payee reviews is conducted on the SSA issued laptops.

b. Ensure all program related written communication with the NAG or SSA occurs using only SSA systems (SSA email, JIRA, RPMT, etc.).

c. Interact with the NAG, SSA, and the public with professionalism and respect.

d. Use SSA systems, software, and equipment (e.g., SSA furnished laptops, printers, scanners, email, Microsoft Teams, and desktop faxing) only for official SSA business performed under this grant. Personal use of SSA systems, software, and equipment is prohibited.

e. Receive SSA written approval before distributing any program-related material to the public.

- P&As must submit public-facing or publicly distributed material to the NAG for preliminary review and approval. The NAG will facilitate submission to SSA for final approval.

Refer to the BPD for procedures for conducting reviews and visits.

PERFORMANCE MEASUREMENT

P&A performance will be assessed by evaluating:

1. The number and types of reviews completed during the grant year in relation to the SSA approved workplan prescribed in the program narrative of the annual grant application. For the purposes of this assessment, "completed" means the review has advanced to the NAG Final Review stage or later in the Representative Payee Monitoring Tool (RPMT). Periodic reviews should be completed within the grant year they are assigned.

   Acceptable performance in this category is defined as:

   a. Completion of 80 percent or more of the overall targeted number of reviews for the current year;
   b. Completion of 80 percent or more of the periodic reviews assigned in the current grant year;
   c. Completion of 100 percent of all periodic reviews assigned in grant years prior to the current grant year.

2. The quality of such reviews as measured by adherence to the processes, procedures and timeframes described in BPD.

   Acceptable performance in this category is defined as:

   a. Less than 20 percent of reviews submitted to the NAG Final Review stage in RPMT are returned for correction.

3. Comparative performance, as measured by evaluating each grantee's outcomes against national averages and program expectations, across key performance measures alongside those of similarly sized organizations.

   Acceptable performance in this category is defined as:

a. Performance outcomes that are consistent with national averages and program expectations, with only minor differences that do not indicate systemic issues or require corrective action.

Data Sources and Reporting Requirements. The primary source of data for the assessment of P&A performance shall be RPMT, which serves as the central repository for the processing and documentation of all casework activities. All casework conducted by grant recipients must be entered into RPMT, thereby ensuring the availability of comprehensive metrics for program evaluation. Grant recipients may, at their discretion, submit additional metrics as part of their annual progress report to further demonstrate program outcomes. Such supplemental metrics may include, but are not limited to, high-profile reviews with significant outcomes, reviews resulting in substantial findings, or examples of reviews that have led to measurable improvements in beneficiaries' quality of life or well-being.

Risk Designation and Specific Conditions. In accordance with 2 CFR 200.206 and 2 CFR 200.208, and at the discretion of SSA, failing to meet the acceptable performance criteria in any category or other relevant criteria may result in a high-risk designation. The imposition of specific conditions will be determined in accordance with these regulations and as described in Attachment I – Notice of Specific Terms and Conditions for Risk Tiered Awards.

The applicability of a risk designation and/or specific conditions will be designated through the initial NOA or a subsequent amendment.

GENERAL TERMS AND CONDITIONS, ADMINISTRATIVE AND NATIONAL POLICY REQUIREMENTS

This award, including all subawards, are subject to the Office of Management and Budget (OMB) Guidance for Grants and Agreements, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards. These regulations can be found at: 2 C.F.R. Part 200.

As applicable to this award, any references to contract(s) means award(s); grantee(s) means recipient(s) or awardee(s); subgrantee(s) means subrecipient(s); subcontract(s) means subaward(s); federal contract information includes confidential information; Project/Program Officer, Contracting Officer's Representative (COR), Contracting Officer (CO), and Grants Management Officer means SSA.

1. Program Income earned must be used for program costs in addition to Federal Funds. Program income is gross income earned by a recipient that is directly generated by a supported activity or earned as a result of the Federal award during the period of performance except as provided in 2 C.F.R. § 200.307 paragraph (f). (See §200.1 Period of performance.) Program income includes but is not limited to income from fees for services performed, the use or rental or real or personal property acquired under Federal awards, the sale of commodities or items fabricated under a Federal award, license fees and royalties on patents and copyrights, and principal and interest on loans made with Federal award funds. Interest earned on advances of Federal funds is not program income. Except as otherwise provided in Federal statutes, regulations, or the terms and conditions of the Federal award, program income does not include rebates, credits, discounts, and interest earned on any of them.

2. This award is subject to the non-procurement debarment and suspension regulations implementing Executive Orders 12549 and 12689, 2 C.F.R., Subtitle

A, Ch. 1, Part 180. These regulations restrict awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in Federal assistance programs or activities. As a recipient of a Federal financial assistance award, each participant in a primary tier covered transaction must comply with this condition and communicate the requirement to 2 persons at the next lower tier with whom the primary tier participant enters into covered transactions.

3. This award is subject to the provisions of 2 C.F.R. § 200.450 Restrictions on Lobbying. The cost of certain influencing activities associated with obtaining grants, contracts, cooperative agreements, or loans is an unallowable cost. Lobbying with respect to certain grants, contracts, cooperative agreements, and loans is governed by relevant statutes, including among others, the provisions of 31 U.S.C. § 1352, as well as the common rule, "New Restrictions on Lobbying" published at 55 FR 6736 (February 26, 1990), including definitions, and the Office of Management and Budget "Government wide Guidance for New Restrictions on Lobbying" and notices published at 54 FR 52306 (December 20, 1989), 55 FR 24540 (June 15, 1990), 57 FR 1772 (January 15, 1992), and 61 FR 1412 (January 19, 1996).

4. This award is subject to the provisions of 2 C.F.R. Part 182, OMB guidance implementing "Government wide Requirements for Drug-Free Workplace Act."

5. The following applies *only* to training materials and other written guidance developed under this grant award:

    a. Definitions

        i. "Data," as used herein, means recorded information regardless of form or the media on which it may be recorded. The term includes computer software and information of a scientific or technical nature. The term does not include information incidental to grant administration such as financial, administrative, cost or pricing or management information and does not include personal identifying information unless informed consent to release such information has been obtained.

        ii. "Computer Software," as used herein, means computer programs, computer data bases, and documentation thereof.

        iii. "Federal Government Purposes," as used herein, does not include the right to use, or authorize others to use data first produced in the performance of this award for commercial purposes. (Commercial purposes being the reproduction of the data, on any medium, that is offered for sale, or the use of the data to produce or to manufacture a product for sale.)

    b. Rights in Data

        i. "Rights in the Recipient of this Award." Except as otherwise provided in the terms and conditions of this award, the recipient shall have the right to and may permit others to copyright, publish, disclose, disseminate and use, in whole or in part, any data first produced in the performance of work under this award.

ii. "Rights in the Federal Government." Except as otherwise provided in the terms and conditions of this award, the Federal Government, and others acting for it or on its behalf shall have the right, and are hereby granted a royalty-free, non-exclusive, irrevocable license throughout the world, to use, reproduce, prepare derivative works, perform publicly, display publicly and distribute to the public, any data, including data copyrighted pursuant to paragraph 5.b.i above, first produced in the performance of work under this award for Federal Government purposes.

c. Access to Data

The recipient of this grant award shall deliver to the Federal Government, as and when requested, a copy of the data to which it has rights thereto under the provisions of paragraph 5.b. above. Such data shall be provided at a cost not-to-exceed the cost of actual reproduction and transmittal.

d. Applicability to Third-Party Transactions

The recipient of this award shall incorporate the above provisions in all third-party transactions involving the development of data under this award, following the guidelines set by this Terms & Conditions and the Business Process Document.

6. The recipient of this grant is responsible for performing the duties detailed in and complying with the requirements of the terms and conditions, the BPD, and SSA guidance.

7. The recipient of this grant shall comply with all data protection, privacy, security, and other requirements in this award, including terms in Attachments A through H to this award.

8. A suspected or confirmed breach of PII (as defined in Attachment A) may lead to the grant being placed in high risk. Additionally, SSA reserves the right to terminate suitability for individuals with PII violations. SSA considers an individual to be an offender when they have violated security and privacy requirements in this award. SSA considers an individual to be a repeat offender when they have violated the agency's PII Policy on more than one occasion. SSA will re-evaluate the individual's suitability specifically when the individual has repeat PII violations or as SSA determines appropriate.

9. Upon suitability approval and at the beginning of each successive grant year, all grantee personnel must complete the annual mandatory Information Security Awareness Training and complete the Security and Privacy Awareness Training Contractor/Affiliate Personnel Security Certification (SSA-222). SSA will issue this training and require certification from the grantee on an annual basis.

10. SSA maintains ownership and all rights over all confidential information at all times. The awardee is not authorized to use confidential information in any other manner outside of this award.

11. The recipient of this grant will assist SSA in complying with the Paperwork Reduction Act (PRA), when applicable. In the event this award involves a requirement to collect or record either information calling for answers to identical questions from 10 or more persons other than Federal employees, or information from Federal employees, which is outside the scope of their employment, for use by the Federal government or disclosure to third parties, the PRA may apply. Therefore, when applicable, no plan, questionnaire, interview guide or

other similar device for collecting information (whether repetitive or single time) may be used without the prior clearance of the Office of Management and Budget (OMB). The SSA Reports Clearance Officer (RCO) is the authorized individual for obtaining the OMB clearance for the agency working with the Program Officer and the grant awardee. The grantee shall not begin any data collection nor expend any funds associated with the data collection until receiving the OMB clearance. Once the SSA RCO receives the OMB clearance, the Program Officer will provide the grantee a notification authorizing the collection of data.

12. Equipment: Property records must be maintained that include a description of the property, a serial number or other identification number, the source of funding for the property (including the FAIN), who holds title, the acquisition date, and cost of the property, percentage of Federal participation in the project costs for the Federal award under which the property was acquired, the location, use and condition of the property, and any ultimate disposition data including the date of disposal and sale price of the property (See 2 C.F.R. 200.313 for further details.) Also note that to the greatest extent practicable, all equipment and products purchased with Federal funds made available in this award should be American made (See Executive Order 13788 for more details.)

13. When issuing statements, press releases, requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or in part with Federal money, all grantees (to include all sub awards under this award) receiving Federal funds, including but not limited to State and local governments and recipients of Federal research grants, shall clearly state (1) the percentage of the total costs of the program or project which will be financed with federal money, (2) the dollar amount of Federal funds for the project or program, and (3) the percentage and dollar amount of the total costs of the project or program that will be financed by nongovernmental sources. The grantee shall ensure the provisions within this paragraph, are included in all sub awards under this award.

14. Prior approval: In performing duties under or as related to this grant, recipients cannot distribute, solicit, or provide to the public any materials, including brochures, articles, websites, forms, data collection request, instructional documents, supplemental instructions, etc. without prior written approval from SSA Program Officials.

    All new content (i.e., not previously approved by SSA in writing), in any form, to be available, solicited, or distributed externally (i.e., outside the entity or organizations) must get prior written approval from SSA.

    Any preapproved SSA.gov publications do not need prior approval from the Program Officer when used without modification.

    The P&A external publications and outreach materials should communicate the P&A's work and should not interpret or otherwise provide instructions on SSA policies, regulations, or guidance for the beneficiaries or representative payees.

Any approved publications shall contain the following disclaimer:

"This document is funded through a Social Security grant agreement. Although Social Security reviewed this document for accuracy, it does not constitute an official Social Security communication."

In all cases, any public-facing or publicly distributed documents, websites, brochures, etc., must also include the phrase "at taxpayer expense". Grantees have some latitude with the phrasing, for example, "We developed this website at U.S. taxpayer expense" or "We published this brochure at U.S. taxpayer expense".

Note, the P&A will route all publications, external and internal (such as training materials, instructions, and guides) to the NAG for review. Questions on publications should be directed to the NAG. If the NAG has questions on the P&A publications, they will forward to the SSA Program Officer.

SSA reserves the right to review any materials to ensure compliance and to revoke any prior approvals at any time.

15. Grant recipients are required to obtain prior approval for budget and program plan revisions in accordance with 2 C.F.R. § 200.308 Revision of budget and program plans. All requests for prior approval including budgetary changes must be submitted as an amendment request via GrantSolutions.gov. Requests must include a concise and comprehensive explanation of the request and how the change(s) meets agency priorities. Grantees can enact requested changes only after receiving written approval from the Social Security Approving Officials.

16. Consistent with 2 C.F.R. 200.308, Social Security requires prior approval of "significant rebudgeting." Significant rebudgeting is defined as the movement of 10% of the Federal award amount or $25,000 and above in total direct costs. Since significant rebudgeting may affect the scope or objectives of a grant, it is subject to Grants Management Officer approval. Grantees must submit a revised budget amendment in GrantSolutions to request approval for changes involving significant rebudgeting. The SSA GMO will subsequently review the request and if approved, will issue an amendment. In the event that the request is not approved, the GMO will provide feedback to the awardee.

    Awardees should note that prior approval is required for but is not limited to: Changes in Key Personnel and Level of Effort, Adding or Deleting Subrecipients (regardless of costs involved), Budget Revisions, Changes in Scope, Carryover Requests (that fall outside the term for the Expanded Authority for Carryover), and No Cost Extensions.

    The requirement to obtain Social Security's prior approval for key personnel changes pertain only to those key personnel in the Notice of Award, regardless of whether the applicant organization designates others as key personnel for its own purposes.

Note: SSA cannot determine who the grantee can hire, however SSA can reject a proposed change in key personnel in our grant and cooperative agreements. Key personnel include Executive Officer, Grant Managers, Project Directors, Attorneys, Project Analyst.

Awardees must request these changes through a note in GrantSolutions and include any supporting documentation, such as subaward agreements, Curriculum Vitae or resumes. Awardees may not proceed with any such change until approval is received from the SSA via GrantSolutions. However, so long as rebudgeting is not related to these actions, awardees may rebudget 10% **but not exceeding $25,000** without Social Security approval.

17. If your award contains a provision for contracting out part of the proposed effort, the Procurement Standards apply: 2 C.F.R. Procurement Standards. Anyone with access to personally identifiable information (PII) must be an employee of the grantee or subgrantee with suitability clearance under the SPSSBA program.

18. Trafficking in Persons: All grantees are required to adhere to: 2 C.F.R. Part 175 Award Term for Trafficking in Persons.

19. Internal Controls 2 C.F.R. § 200.303:
The grantee must establish, document, and maintain effective internal control over the Federal award that provides reasonable assurance that the recipient is managing the Federal award in compliance with Federal statutes, regulations and the terms and conditions of the award. These internal controls should be in compliance with guidance in" Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States or the "Internal Control Integrated Framework", issued by the Committee on Sponsoring Organizations of the Treadway Commission. Comply with the U.S. Constitution, Federal statutes, regulations, and the terms and conditions of the Federal award. (a) Evaluate and monitor the recipient's compliance with statutes, regulations and the terms and conditions of Federal awards. (b) Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings. (c) Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the recipient considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality. [78 FR 78608, Dec. 26, 2013, as amended at 79 FR 75883, Dec. 19, 2014]

20. The grantee must maintain written standards of conduct covering conflicts of interest and governing the actions of its employees engaged in the selection, award and administration of contracts. No employee, officer or agent may participate in the selection, award or administration of a contract supported by a Federal award if he or she has a real or apparent conflict of interest. Such a conflict of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner or an organization which employs or is about to employ any of the parties indicated herein, has a financial or other interest or a tangible personal benefit from a firm considered for a contract. The officers, employees and agents of the grantee may neither solicit nor accept gratuities,

favors or anything of monetary value from grantees or parties to subcontracts. However, grantees may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. **The standards of conduct must provide for disciplinary actions to be applied for violations**. Note: The NAG must notify SSA of any conflict of interests identified by the NAG or P&As.

21. The grantee must maintain written standards of conduct covering conflicts of interest (COI) and governing the actions of the grantee organization or its staff (employees, or sub awardees/contractors) when prior relationships between the individual employee/staff and the interviewees (i.e., beneficiary, payee, legal guardian, or third party) affect that staff's ability to conduct their work under this grant fairly and effectively. The grantee must ensure all personnel are trained on COI. The grantee must submit the conflict-of-interest policy to SSA upon request.

    The grantee must report to SSA any potential COI concerning the NAG or any P&A within 14 calendar days of the discovery along with the approach for resolving the COI. Upon notice from the recipient of a potential COI and the approach for resolving it, SSA will make a determination regarding the effectiveness of these measures within 30 days of receipt of notice unless a longer period is necessary due to the complexity of the matter. The grantee must not take further action on the matter until SSA notifies the NAG/P&A.

22. Pursuant to Executive Order 13513, "Federal Leadership on reducing Text Messaging While Driving," 74 Fed. Reg. 51255 (October 1, 2009), SSA encourages recipients and subrecipients to adopt and enforce policies banning employees from text messaging while driving any vehicle during the course of performing work funded by this grant, and to establish workplace safety policies and conduct education, awareness and other outreach to decrease crashes caused by distracted drivers.

23. Whistleblower Protections 2 C.F.R. 200.217:
    An employee of a recipient or subrecipient must not be discharged, demoted, or otherwise discriminated against as a reprisal for disclosing to a person or body described in paragraph (a)(2) of 41 U.S.C. 4712 information that the employee reasonably believes is evidence of gross mismanagement of a Federal contract or grant, a gross waste of Federal funds, an abuse of authority relating to a Federal contract or grant, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a Federal contract (including the competition for or negotiation of a contract) or grant. The recipient and subrecipient must inform their employees in writing of employee whistleblower rights and protections under 41 U.S.C. 4712. See statutory requirements for whistleblower protections at 10 U.S.C. 4701, 41 U.S.C. 4712, 41 U.S.C. 4304, and 10 U.S.C. 4310

NONCOMPLIANCE & TERMINATIONS

24. The following Terms and Conditions are for Remedies for Noncompliance as per 2 C.F.R. § 200.339: Remedies for noncompliance. If a recipient fails to comply with Federal statutes, regulations or the terms and conditions of a Federal award, the Federal awarding agency or passthrough entity may impose additional conditions, as described in 2 C.F.R. § 200.208 Specific conditions. If the Federal awarding agency or passthrough entity determines that noncompliance cannot be remedied by imposing additional conditions, the Federal awarding agency or passthrough entity may take one or more of the following actions, as appropriate in the circumstances:

    i. Temporarily withhold cash payments pending correction of the deficiency by the recipient or more severe enforcement action by the Federal awarding agency or pass-through entity
    ii. Disallow (that is, deny both use of funds and any applicable matching credit for) all or part of the cost of the activity or action not in compliance.
    iii. Wholly or partly suspend or terminate the Federal award.
    iv. Initiate suspension or debarment proceedings as authorized under 2 C.F.R. part 180 and Federal awarding agency regulations (or in the case of a pass-through entity, recommend such a proceeding be initiated by a Federal awarding agency).
    v. Withhold further Federal awards for the project or program.
    vi. Take other remedies that may be legally available.

25. The following are Terms and Conditions for Termination per 2 C.F.R. § 200.340

    a) The Federal award may be terminated in part or its entirety as follows:
        i. By the Federal agency or pass-through entity, if a recipient or subrecipient fails to comply with the terms and conditions of a Federal award;
        ii. By the Federal agency or pass-through entity with the consent of the recipient or subrecipient, in which case the two parties must agree upon the termination conditions. These conditions include the ffective date and, in the case of partial termination, the portion to be terminated;
        iii. By the recipient upon sending to the Federal agency or pass-through entity written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if the Federal agency or pass-through entity determines that the remaining portion of the Federal award will not accomplish the purposes for which the Federal award was made, the Federal agency or pass-through entity may terminate the Federal award in its entirety; or
        iv. By the Federal awarding agency or pass-through entity pursuant to terms and conditions of the Federal award, including, to the extent authorized by law, if an award no longer effectuates the program goals or agency priorities.

    b) A Federal agency or pass-through entity must clearly and unambiguously specify all termination provisions in the terms and conditions of the Federal award.

c) When a Federal agency terminates a Federal award prior to the end of the period of performance due to the recipient's material failure to comply with terms and conditions of the Federal award, the Federal agency must report the termination in *SAM.*gov. A Federal agency must use the Contractor Performance Assessment Reporting System (CPARS) to enter information in *SAM.*gov.

(1) The information required under paragraph (c) of this section is not to be reported to in *SAM.gov* until the recipient has either:

(i) Has exhausted its opportunities to object or challenge the decision, see §200.342; or

(ii) Has not, within 30 calendar days after being notified of the termination, informed the Federal awarding agency that it intends to appeal the decision to terminate.

(2) If a Federal awarding agency, after entering information into *SAM.gov*, subsequently:

(i) Learns that any of that information is erroneous, the Federal agency must correct the information in the system within three business days.

(ii) Obtains an update to that information that could be helpful to other Federal agencies, the Federal agency is strongly encouraged to amend the information in the system to incorporate the update in a timely way.

(3) The Federal agency must not post any information that will be made publicly available in the non-public segment of *SAM.gov* that is covered by a disclosure exemption under the Freedom of Information Act (FOIA). When the recipient asserts within seven calendar days to the Federal agency that posted the information that a disclosure exemption under FOIA covers some of the information made publicly available, the Federal agency that posted the information must remove the posting within seven calendar days of receiving the assertion. Before reposting the releasable information, the Federal agency must resolve the issue in accordance with the agency's FOIA procedures.

d) When the Federal award is terminated in part or its entirety, both the Federal agency or pass-through entity and the recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. § 200.344 and § 200.345.

PROGRAM PROGRESS, FINAL REPORT AND FINANCIAL STATUS REPORTING

26. Annual Progress Reports describing accomplishments and activities.

Progress Reports are due by the following dates:

Reporting Period:	Due No Later Than:
August 1 – July 31	August 31

You must submit all Progress Reports via the online Performance Progress Report (PPR) online module within GrantSolutions.gov by the due dates.

It is expected that reports will include data appropriate to this stage of project development and in sufficient detail to provide a clear idea and summary of work and accomplishments to date.

Grantees must submit the Annual Progress Report using the following format:

a. Representative Payee Reviews: This section should address number and types of reviews finished during the prior 6-month period. Include pre-review activities and program challenges and accomplishments.

b. Staffing: (time and expense to create, advertise and hire positions)

c. Security Clearance: (time spent in hours or percentage going through the SSA suitability process and time spent going through the credentialing and laptop issuing; the number of staff with suitability and the number of staff with credentials)

d. Training received: (time spent in hours or percentage preparing for and attending NAG annual meeting | ex. time spent at rep payee session at July fiscal managers meeting | time spent at the NAG CEO Mtg.)

e. Participation at conferences and on calls: (time spent in hours or percentage on NAG live and recorded trainings | time spent on SSA led training webinars | also time on quarterly CEO calls)

f. Efforts on developing leads for P&A initiated reviews: (time spent in hours or percentage – activities and outcome. Include situations that affect the normal progress and standard workflow; any significant problems/challenges that the grantee encountered and how it was resolved/corrected; major issues requiring assistance; oversight provided by the P&A management; workload/technical training provided to the reviewer; results of internal quality checks performed).

g. Orientation for P&A staff: (Agency orientation of rep payee staff | any hands-on training related to the monitoring payees or interviewing beneficiaries)

h. Other: (general support issues | time spent traveling to SSA field offices | working with SSA on equipment issues)

i. Equipment: A list of SSA issued equipment possessed by the P&A. Please include the following information:
   - description of the property (i.e., laptop, printer, scanner, laptop bag)
   - count(s) of the equipment
   - serial number (or other identification number)
   - Netname for laptop equipment
   - location of the equipment

j. Work Plan:
   - End of Year (August Report): Please provide a summary of the Representative Payee Program for the full grant year. This section should address total number and types of reviews finished for the full grant year, including program challenges and accomplishments.

Federal Financial Reports (SF425): The SF425 (FFR), instructions, as well as our Tip Sheet for completing the SF425 are available to download from the Frequently Asked Questions (FAQs) section of our website at our ssa.gov website.

The following dates are based on the OMB SF425 instructions:

March 31
June 30
September 30
December 31

FFRs must be completed using the online Federal Financial Report module within GrantSolutions.gov and must include all necessary corresponding documentation. The online report is cumulative and is due one month after the Report Period End Date.

27. SPSSBA legislation, Section 101 [42 U.S.C. 405] paragraph (III)(i): "Funds provided to protection and advocacy system through a grant under clause (i) for a 1-year period shall remain available through the end of the following 1-year period."

    Therefore, any unspent FY24 (GY7) funds on this award will be de-obligated after July 31, 2026.

    All payment requests must include the full corresponding grant number for the fiscal year from which the grantee is requesting funds. For example, a payment request for FY24 funds must include the full grant number.

    Funds are not presently available for performance under this grant beyond July 31, 2026. The government's obligation for performance of this grant beyond that date is contingent upon the availability of appropriated funds from which payment for grant purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this grant in excess of the funds listed herein or beyond July 31, 2026. Grantees will be notified in writing by the Office of Acquisitions and Grants regarding future funding.

28. Subaward Reporting.
    This award is subject to the provisions of OMB regulation 2 C.F.R. Part 170, Reporting Subaward and Executive Compensation Information. The Federal Funding Accountability and Transparency Act requires all prime grantees to report specific subawards. The regulation is available on our website. SSA will monitor this requirement on USASpending.gov. On March 8, 2025, FSRS.gov was retired, and all subaward reporting, data,

and functionality are now on www.sam.gov.

29. Federal Awardee Performance and Integrity Information System (FAPIIS).
SSA will, in accordance with 2 C.F.R. § 200.205 review the FAPIIS to determine if a grantee is qualified to receive an award. Grantees should review the information in FAPIIS about their entity before submitting a continuation application. In addition to reviewing FAPIIS, agency officials will verify grantees' eligibility through the System for Award Management Exclusion Extract (SAM.gov).

FEDERAL AWARDING AGENCY CONTACT(S)

For matters related to the grant award, submit an email with the subject: H.R. 4547 - Strengthening Protections for Social Security Beneficiaries Act 2018 (SPSSBA) -- SPS23000XXX (P&A Grant Number).

SPSSB Grant Contacts
Grant Management Officer:
Daniel Dennis
Social Security Administration
Strategic Sourcing
1540 Robert M. Ball Bldg.
6401 Security Blvd
Baltimore, Maryland 21235
Daniel.Dennis@ssa.gov

Grants Management Officer:
Audrey Adams
Social Security Administration
Strategic Sourcing
1540 Robert M. Ball Bldg.
6401 Security Blvd
Baltimore, Maryland 21235
410-965-9469
Audrey.Adams@ssa.gov

Program Officer:
Each P&A will have an assigned Federal Program Officer for this project. If you have any questions regarding the programmatic aspects of this award, please contact your agency-assigned Program Officer.

Social Security Administration
Representative Payee
6401 Security Blvd
Mail Stop: 1620
Baltimore, Maryland 21235

SPSSBA.Rep.Payee.Grants@ssa.gov

OTHER INFORMATION

Payment and Project Costs:

The grantee agrees that it will only charge allowable costs incurred to the award during this period of performance. The grantee agrees to relate its financial charges to the approved work products and accomplishments.

Upon request by the agency, the grantee agrees to provide the agency with all cost and expense data and information related to its work on special projects. Further, upon request, the grantee agrees to provide the agency with all cost and expense data for any of its authorized subrecipients for work on funded projects.

Payment Arrangements:

All drawdowns must be completed through the Automated Standard Application Payments (ASAP). If you have issues with payments, please contact: dcms.ofppi.df.administrative.grants@ssa.gov in the Division of Financial Reporting, Debt Management, & Treasury Reporting (FRTRPT). Recipients must include "ASAP Assistance" and ASAP ID# in the subject line of each email.

Grantees must maintain written procedures that minimize the time elapsing between the transfer of funds and the disbursement and financial management systems that meet the standards for fund control and accountability as established in 2 C.F.R. 200. See 2 C.F.R. §305 for additional guidance on payments.

All Request for Advance or Reimbursement SF-270s must be signed by the authorized certifying official and emailed to SSA prior to the drawdown of funds.

The signed SF-270 must be emailed to: FM.Acct.FS.Administrative.Grants@ssa.gov for review by SSA/DCAR. Recipients must include "SF-270" and their SPS23XXXXX-0X in the subject line of the

(End Clause)

Attachment A – SSA Information Security and General Privacy Requirements (AUG 2024)

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 recipient for, or otherwise obtained by the recipient 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 recipient as a result of this award. 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 grantee 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, Recipient, 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 Recipient 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 Recipient employee's official place of work that is in the Recipient'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 Recipient 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.

1. Information Security and Privacy Governance.

The Recipient shall comply with the laws, regulations, directives, policies, standards, and guidelines listed in – *Attachment H- Privacy Requirements*, 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 Recipient 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 Recipient must comply with, the Recipient shall seek clarification from the COR.

The Recipient 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.

2. Subrecipients.

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

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

The Recipient 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 Recipient shall not subcontract the operational configuration and control of any system used to process or store federal information.

Note: The subrecipient is required to notify the prime Recipient in instances where the language states the recipient shall notify the agency or COR.

3. Indemnification.

The Recipient 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 Recipient's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into federal information. The Recipient agrees to waive all defenses that may be asserted for its benefit, including (without limitation) the Recipient'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 Recipient's unauthorized disclosure of trade secrets, copyrights, grant 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 Recipient's unauthorized introduction of any libelous or other unlawful matter into federal information. The recipient agrees to waive all defenses that may be asserted for its benefit, including without limitation the agency Recipients 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 Recipient shall furnish to the agency, when requested by the CO, all evidence and information in the Recipient's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Recipient; 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 Recipient.

d. The provisions of this paragraph do not apply unless the agency provides notice to the Recipient as soon as practicable of any claim or suit, affords the Recipient an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Recipient'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 Recipient 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 Recipient, unless required by final decree of a court of competent jurisdiction.

4. Safeguarding Federal Information and Information Systems.

The Recipient 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 Recipient on behalf of SSA regardless of location. In addition, if the Recipient 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 Recipient 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 Recipient is responsible under this contract or to which the Recipient 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.

5. 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	[x] Moderate	[ ] High
Integrity:	[ ] Low	[x] Moderate	[ ] High

Availability:	[ ] Low	[x] Moderate	[ ] High
Overall Risk Level:	[ ] Low	[x] 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.*

6. 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 [X] Yes PII

PII Confidentiality Impact Level has been determined to be:

[ ] Low [x] Moderate [ ] High

7. Minimum Security Baseline.

The Recipient shall ensure that all federal information systems or services it provides shall meet or exceed the minimum-security baseline corresponding to a moderate-impact system under the latest revision of NIST Special Publication 800-53.

8. Controlled Unclassified Information (CUI).

The Recipient 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 Recipient 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 Recipient 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 Recipient 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 [x] Yes CUI

CUI Category (e.g. PII, FTI, etc.)

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.

9. Protecting CUI on Nonfederal Information Systems.

The Recipient 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 Recipient shall ensure that all nonfederal information systems, which the Recipient is responsible for, that process or store CUI meet or exceed the security controls as specified by NIST SP 800-171.The Recipient 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 grantee 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.

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

The Recipient 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 recipient 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 Recipient shall assist the agency with completing documentation required for a PIRA for the system or information. The recipient shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than ***30*** days after the documentation or information has been requested by the COR.
2. The Recipient shall assist the COR or designee in reviewing the PIRA at least every 30 days 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.

11. Digital Identity Risk Assessment (DIRA)

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

The Recipient 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

Recipient 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 Recipient shall assist SSA with completing documentation required for a DIRA for they system. The recipient shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than 30 days after the documentation or information has been requested by the COR.
b. The Recipient shall assist the COR or designee in reviewing the DIRA at least every 30 days 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 Recipient 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. Recipient 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 recipient's representative for the contract of the violation.

PHYSICAL LOCATION AND DATA JURISDICTION REQUIREMENTS

1. The Recipient 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 Recipient 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 Recipient'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 Recipient 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 recipient shall provide physical access to the hosting facility for inspection.
3. At the request of the CO, the Recipient 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 recipient facility where federal information is located. If the federal information is co-located with nonfederal information, the Recipient 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 Recipient's involvement.
4. The Recipient 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 Recipient shall maintain a complete inventory of all hardware and software used in the execution of the contract, including model or version numbers. If the Recipient is processing, storing, or transmitting PII/CUI, the Recipient must indicate in the complete inventory which systems process that information. The Recipient shall provide this inventory information to the CO or COR, upon request.
2. **Manufacturer Support**. The Recipient must ensure that all software used in execution of this contract is within one major version of the current version. The Recipient must ensure that all software and hardware used in execution of this contract has manufacturer support. The Recipient must retire or upgrade all software and systems that have reached end-of-life.
3. **Standard for Encryption of electronic information**. The Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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.

   Recipients 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 Recipient shall comply with all Binding Operational Directives (BOD). (https://cyber.dhs.gov/directives/)

9. **Secure Email Requirements**. The Recipient's corporate or organizational email system is deemed not to be secure. Therefore, the Recipient 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 Recipient 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 Recipient'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 Recipient and its employees are expected to conduct business operations under this contract using the Recipient'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 Recipient's corporate or organizational email system has been deemed by SSA to be secure.

10. **Data Access and Use Requirements**. The Recipient shall:
    a. **NOT** access, use, or disclose confidential information, except as necessary to execute the contract requirements.

    b. Only disclose confidential information to authorized Recipient personnel who need the information or equipment in the performance of work under this contract. The Recipient 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 Recipient receives a request, subpoena, or court order for agency confidential information, the Recipient will promptly provide (within two business days) the CO notice of such request. The Recipient will provide the agency with the information or tools required for the agency to respond to the request, if necessary. The Recipient shall refer the requester to the agency. The Recipient will not provide a requester any agency confidential information unless authorized by the agency. The Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient's scanning results and, at agency discretion, accept those in lieu of agency performed vulnerability scans.

e. At the direction of the COR, within *60* days following the agency's final acceptance of the work under this contract or expiration or termination of this contract, whichever occurs first, the Recipient 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 Recipient 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 Recipient-owned systems including backup systems and media used during contract performance, in accordance with NIST SP 800-88, *Guidelines for Media Sanitization.* The Recipient must provide a certification to the COR that the Recipient properly sanitized, purged, and destroyed electronic and physical records of SSA information obtained in execution of this contract.

13. **Audit Record Retention**. The Recipient 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 Recipient 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 recipient 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 Recipient 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 Recipient 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 recipient shall assess the validity of all current applicable security controls. Additionally, at least annually, the Recipient 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 Recipient's responsibility to ensure system security and privacy controls are operating effectively on an ongoing basis. The Recipient shall ensure system security and privacy controls are operating effectively on an ongoing basis.

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

1. The Recipient 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 Recipient 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 Recipient's organization has responsibility for reporting the breach or incident to the agency. The Recipient must follow incident reporting and breach protocols as specified by the agency.

3. The Recipient 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 Recipient 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 Recipient personnel with a need for the information to respond to and take action to prevent,

minimize, or remedy the breach or incident. The Recipient 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 Recipient's confidential information breach and incident reporting process shall ensure that disclosures are made consistent with these requirements.

5. The Recipient 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 Recipient 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 Recipient has contacted or been contacted by any external organizations (i.e., other agencies, law enforcement, press, etc.); and

    Any other pertinent information.

6. The Recipient 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 Recipient facilities during a breach or incident investigation.

ADDITIONAL INFORMATION SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED SOLUTIONS

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

1. **FEDRAMP Authorization Requirements**. The Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient's implementation status as documented in the Security Assessment Report and related continuous monitoring artifacts. In addition, the Recipient 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 Recipient's expense, before SSA issues an ATO.

4. **Physical Access Records.** The Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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 Recipient 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.

For devices with severe character limitations: *I've read & consent to terms in IS user agreement.*

9. **Facility Inspections.** The Recipient 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 Recipient's plan for addressing or resolving of the audit results shall be shared with the COR within 20 days of the Recipient'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 Recipient 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 Recipient 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 Recipient shall also make appropriate personnel available for interviews and provide all necessary documentation during these reviews.

11. **Maintenance.** The Recipient 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 Recipient'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 Recipient'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 Recipient's operating environment. Furthermore, the Recipient 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 Recipient's operating environment and serving the agency are compatible with existing systems and architecture of the agency.

12. **Continuous Monitoring.** The Recipient 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 Recipient will provide the report to the agency within 10 business days.

13. **Penetration Testing.** The SSA reserves the right to perform penetration testing on Recipient's systems, facilities, or cloud services used by the Recipient to deliver services to the SSA. If the agency exercises this right, the Recipient 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 Recipient 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 Recipient to the designated POA&M and mitigated within the agreed upon timelines. SSA will determine the risk rating of vulnerabilities using FedRAMP baselines.

(End Clause)

2352.224-2A – Protecting and Reporting the Loss of Personally Identifiable Information (MAY 2026)

(a) *Definitions.*

The following terms are defined for the purposes of this clause:

"Agency" means the Social Security Administration (SSA).

"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 personally identifiable information (PII); or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII 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 PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII 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 PII, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;
- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
- An information technology system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

"Employee(s)" means individual(s) under a direct employee-employer relationship with the Contractor, where the Contractor has the power or right to control and direct the individual in the material details of how work is to be performed.

"Handling of PII" or "handle(s) PII" means accessing, using, creating, collecting, processing, storing, maintaining, disseminating, disclosing, disposing, or destruction of PII, as defined in this clause.

"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.

"Personally identifiable information" (PII) means 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.

"Primary agency contact" means the SSA Contracting Officer's Representative (COR), or, for indefinite delivery contracts with individual orders issued against the contract, e.g., task-order contracts, the order's Task Manager, if one has been assigned. The COR may have one or more designated alternates to act for the COR when the COR is unavailable. If neither the COR nor the designated alternate is available, the alternate shall be considered a responsible agency manager in the office.

"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. 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.

"Suspected breach" means PII that, among other possibilities, has been lost or stolen, or accessed in an unauthorized fashion, but it is not yet confirmed that the PII has been compromised to meet the level of a breach.

"Transport(ing)" or "transported" means the physical taking or carrying of PII from one location to another. For the purpose of this clause, the term does not include shipping by a common or contract carrier (as defined in Federal Acquisition Regulation (FAR) section 47.001), shipping by the U.S. Post Office, or electronic transmission. [*Contracting Officer—Insert a sentence providing for a cross reference to location of contract terms and conditions on shipping and/or electronic transmission, if applicable.*]

(b) *Responsibility for Safeguarding PII.*

(1) The Contractor shall comply with applicable limitations on use, treatment, and safeguarding of PII under the Privacy Act of 1974 (5 U.S.C. § 552a); the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related National Institute of Standards and Technology guidelines; the Paperwork Reduction Act, 44 U.S.C. § 3501-3521; the E-Government Act of 2002, 44 U.S.C. § 3501 note; Office of Management and Budget (OMB) guidance relating to handling of PII, including OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"; SSA privacy and security policies and procedures relating to handling of PII; and other Federal laws governing handling of PII.

(2) The Contractor shall establish, maintain, and follow its own policies and procedures to protect the confidentiality of PII (PII policies and procedures) in accordance with the laws, policies, and requirements referenced in this clause and elsewhere in the contract. The Contractor's PII policies and procedures shall include safeguards to protect PII from loss, theft, or inadvertent disclosure and breach procedures.

(3) The Contractor shall restrict handling of PII to only those authorized employees who need it in connection with the performance of work under this contract.

(4) Unless authorized by this contract or otherwise in writing by SSA, the Contractor shall not publish, disclose, release, or otherwise disseminate PII, internally or externally.

(5) The Contractor shall inform its employees who will or may handle PII of their individual responsibility to safeguard it. In addition, the Contractor shall educate and train employees as required by FAR 24.301 and enforce employees' compliance with the Contractor's PII policies and procedures and other requirements relating to handling of PII in this contract. SSA may require the Contractor to provide evidence of the performance of training and the content of the training.

(6) Additional policies, procedures, and requirements involving the handling of PII may be prescribed elsewhere in this contract, including but not limited to information security policies. The Contractor shall follow all such policies, procedures, and requirements. If contract performance calls for the Contractor handling of PII in a manner not addressed in this clause or elsewhere in the contract that may cause a security question or concern, the Contractor shall seek clarification and direction from the agency, prior to commencing the handling of PII in question. [*Contracting Officer—Insert a sentence providing for a cross reference to location of contract terms and conditions on additional security policy and procedure not already discussed or referred to in this clause, if applicable.*]

(c) *Safeguarding Requirements.*

(1) The Contractor is responsible for safeguarding PII at all times. The Contractor shall ensure that PII remains under the immediate supervision and control of authorized employees in a manner that will protect the confidentiality and integrity of PII. Examples of proper safeguarding include, but are not limited to: maintaining the confidentiality of each employee's individual password (by not sharing the password with any other individual or entity and not writing it down); verifying the identity of individuals before disclosing information to them; preventing others in the area from viewing PII on one's computer screen; consistently locking or logging off one's workstation when one is away; and ensuring that PII is appropriately returned or, upon receiving the agency's approval, destroyed when no longer needed. The Contractor may use its internal policies and practices, non-disclosure agreements, system security requirements or any other means to accomplish its safeguarding responsibilities.

(2) *Transporting PII Outside a Secure Area/Secure Duty Station.*

(i) The Contractor shall safeguard equipment, files, or documents containing PII when transporting information from a secure area/secure duty station. The Contractor shall ensure that the laptops and other electronic devices/media being used to transport PII are encrypted and password protected. The Contractor shall ensure that the encryption and password protection are in accordance with any agency-prescribed standards or policies, which shall be communicated separately from this clause. [*Contracting Officer—Insert a reference, if available, to where these standards or policies can be found.*] The Contractor shall use reasonable protection measures when transporting PII, e.g., storing files in a locked briefcase, not leaving files and/or equipment in plain view.

(ii) The Contractor shall ensure that its PII policies and procedures address transporting PII outside a secure area and emailing PII to and from non-SSA email addresses. The Contractor shall provide employees,

upon or immediately prior to their commencing work on the contract, with contact information and instructions relating to PII breaches and incidents, based on the Contractor's security/PII loss incident policy and procedures. (If the preceding requirement is introduced to the contract under a contract modification, the Contractor shall ensure employees are provided this information and instructions within 10 working days of the modification.) The Contractor shall periodically remind employees of the foregoing information and instructions per the regular training requirements at (d)(1), below. (NOTE: Agency-prescribed contact information and instructions for reporting lost or possibly lost PII are discussed in paragraph (d) below.) SSA may require that the Contractor present evidence of compliance with these provisions.

(iii) *Tracking PII-containing material (files, documents, etc.).*

(A) Unless the PII is being transported for disposal pursuant to the contract per (c)(3) below, or SSA grants an exception per (c)(2)(iii)(D), below, the Contractor shall take appropriate and necessary action to ensure that the PII-containing material, such as file(s) or document(s) being physically transported or transmitted electronically outside the secure area/secure duty station, are tracked through a log. The PII-containing material shall be logged out prior to transport as well as logged back in upon return. The Contractor can establish any mechanism for tracking as long as the process, at a minimum, provides for the following information to be logged:

(1) first and last name of the employee taking/returning the material;

(2) the identification of the PII-containing material, such as the name of the file(s) or document(s) containing PII;

(3) the media used to transport the PII (e.g., electronic, such as laptop, portable drive, compact disc/digital versatile disc (CD/DVD), or email—be as specific as possible; paper, such as paper file folders or printouts);

(4) the reason he/she intends to transport the PII-containing material;

(5) the date he/she transported the PII-containing material from the secure area/secure duty station;

(6) the date the PII-containing material is due to be returned to the secure area/duty station. See subparagraph (c)(2)(iii)(B), immediately below.

(7) the approver's name and phone number.

(8) the actual return date of the PII-containing material.

(B) Materials shall be returned or, when authorized by paragraph (c)(3), documented as destroyed, within 90 days of removal from the office or have Contractor supervisory approval for being held longer.

(C) The log shall be maintained in a secure manner. Upon request by the agency, the Contractor shall provide the information from the log in a format (e.g., electronic or paper) that can be readily accessed by the agency. The Contractor shall retain the log in accordance with General Records Schedule 4.2, Information Access and Protection Records, Item 40 (disposition authority DAA-GRS-2016-0002-0004).

(D) SSA may relieve the Contractor of having to comply with these logging requirements for certain transmissions when the Contractor is engaged in routine and secure transmission of PII, and SSA determines that there are appropriate security controls in place to track the data through other means.

(3) *Return and/or Disposal of PII.* The Contractor shall return and/or dispose of the PII when the PII is no longer required for performance of this contract, e.g., upon contract completion, per agency direction and requirements. The marked statement(s) below apply to this contract: [*Contracting Officer: Mark all that apply below.*]

[ ] (i) This contract entails the return of PII.

[ ] (ii) This contract entails the disposal of PII. The Contractor shall follow the procedures described in [*Contracting Officer: Fill in reference to appropriate section, paragraph, article, etc., of the contract as applicable. Page numbers are optional.*]

(4) *Emailing PII.* 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 employees email PII using only the following procedures in (i) - (ii), below:

(i) *Sending from an SSA email address*. If employees have been given access to the SSA email system, they may use it to send email messages containing PII 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 PII only if the PII is entirely contained in an encrypted attachment. The Contractor shall encrypt PII in accordance with OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).

(ii) *Sending from a non-SSA email system*. If employees are using the Contractor's own or any other non-agency email system (e.g., Yahoo!, Gmail), they may send email messages transmitting PII only if the PII is entirely contained in an encrypted attachment, per OMB Circular A-130; none of the PII may be in the body of the email itself or in an unencrypted attachment. When emailing from such systems, this procedure applies when emailing PII 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 PII.

SSA may grant written exceptions to compliance with the email requirements in paragraph (c)(4) above when the Contractor's corporate or organizational email system has been deemed by SSA to be secure.

(d) *Procedures for Reporting PII Breach or Incident*. The agency has its own reporting requirements for PII breaches or incidents. The purpose of the following paragraphs is to ensure that the Contractor meets the requirements and shares breach or incident information appropriately. The Contractor's report of a breach or incident will not, by itself, be interpreted as evidence that the contractor failed to provide adequate safeguards for PII.

(1) *Contractor Responsibility.* In addition to establishing and implementing its own internal procedures referenced in paragraph (b), above, the Contractor shall provide regular training (at least annually and when new employees commence work) for contractors on how to identify and report a breach or incident and take

reasonable actions to implement agency-prescribed procedures described in paragraph (d)(3) below for reporting PII breaches or incidents. These include training employees handling PII about these procedures, including how to identify and report a PII breach or incident, and otherwise taking appropriate and necessary steps to enforce their compliance in carrying them out. The Contractor shall cooperate and exchange information with agency officials, as determined necessary by the agency, in order to report and manage a suspected or confirmed breach or incident effectively. The Contractor shall maintain capabilities to determine what agency information was or could have been accessed and by whom, be able to construct a timeline of user activity, determine methods and techniques used to access agency information, and identify the initial attack vector. The Contractor shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with OMB memorandum M-17-12 and agency guidance and breach procedures to assist with responding to a breach or incident. SSA may require evidence of compliance with this guidance.

(2) *Potential Need for Immediate, Direct Reporting by the Employee.* The agency recognizes that Contractor employees will likely make the initial discovery of a PII breach or incident. When an employee becomes aware or suspects that PII has been lost or compromised, he/she is required to follow the Contractor's established security/PII breach/incident reporting process (see paragraph (d)(1), above). The Contractor's reporting process, along with the agency's (see paragraph (d)(3) below), shall require the Contractor, and not necessarily the employee, in such circumstances to notify the agency of the breach or incident. However, the Contractor shall inform each employee handling or potentially handling PII that he/she must be prepared to notify outside authorities directly and immediately as described in paragraph (d)(3)(v) below, if, shortly following the breach or incident or discovery of the breach or incident, he/she finds it evident that neither an appropriate Contractor nor the agency manager/contact can be reached. The Contractor shall emphasize to the employee that timeliness in reporting the incident is critical.

(3) *Procedures*.

(i) When a Contractor employee becomes aware of or suspects a PII breach or incident, the Contractor, in accordance with its incident reporting process, shall provide immediate (as soon as possible and without unreasonable delay) notification of the breach or incident to the primary agency contact. If the primary agency contact is not readily available, the Contractor shall immediately notify the contact's alternate. (**See the worksheet in agency-specific clause H2352.224-2b, below, for the identity of the designated primary and alternate agency contacts.**) The Contractor shall act to ensure that each employee, prior to commencing work on the contract, has been given information as to who the primary and alternate agency contacts are and how to contact them. In addition, the Contractor shall act to ensure that each employee promptly receives any updates on such information, as they are made available. Whenever the employee removes PII from a secure area/secure duty station, he/she shall comply with the Contractor's security policies, including having on hand the current contact information for the primary agency contact and at least one alternate.

(ii) The Contractor shall provide the primary agency contact or the alternate, as applicable, updates on the status of the reported PII loss or compromise as they become available but shall not delay the initial report.

(iii) The Contractor shall provide complete and accurate information about the details of the PII breach or incident to assist the agency contact/alternate, including the following information:

(A) Contact information;

(B) A description of the PII breach or incident (i.e., nature of the breach, scope, number of

files or records, type of equipment or media, etc.) including the approximate time and location of the loss;

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

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

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

(F) Whether the Contractor or its employee has filed any other reports (i.e., Federal Protective Service, local police, and agency reports); and

(G) Any other pertinent information.

(iv) The Contractor may use the worksheet following this clause to gather and organize information quickly about the incident. The Contractor shall ensure that each employee with access to PII under the contract, prior to accessing the PII, has a copy of the worksheet with its instructions (see agency-specific clause 2352.224-2b), and particularly when transporting PII from a secure duty station.

(v) There may be rare instances (e.g., outside of business hours) when the Contractor is unable to reach either the primary agency contact or the alternate immediately. In such a situation, the Contractor shall immediately call the agency's Enterprise IT Customer Service Desk (ECSD) toll-free at 1-877-697-4889 to file the initial report directly, providing the information in (d)(3)(iii) above and as requested by the ECSD (again, the worksheet in agency-specific clause 2352.224-2b may be used to collect and organize the information prior to (and/or during) the call). Overall, during this time, the Contractor shall cooperate as necessary with the ECSD or any of the other external organizations described in (d)(3)(iii) above. This procedure applies to all Contractor employees. The Contractor shall ensure its internal procedures and PII breach/incident training make clear to employees these responsibilities. Reports to the ECSD should not be delayed because an employee could not reach the Contractor's management.

(vi) The Contractor and its employee(s) shall limit disclosures about PII involved in a breach or incident to only those SSA and Contractor employee(s) with a need for the information in order 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 PII involved may only be disclosed to such authorities and third parties as Federal law permits. The Contractor shall not, without SSA approval, publicly disclose information about PII involved in a breach or incident or SSA's involvement in a breach or incident. The Contractor shall not, without SSA approval, notify individuals affected by the PII breach or incident. The Contractor's PII breach and incident reporting process shall ensure that disclosures are made consistent with these requirements. As used in this paragraph, the term PII references only PII covered by this clause.

(e) *Additional Contractor Responsibilities When There Is a Suspected or Confirmed Breach.*

(4) The Contractor shall have a formal security/PII breach or incident reporting process in place that outlines appropriate roles and responsibilities, as well as the steps that must be taken, in the event of a security/PII breach or incident. The plan shall designate who within the Contractor's organization has

responsibility for reporting the PII breach or incident to the agency.

(5) In the event of a PII breach or incident, the Contractor shall take immediate steps to address consequential security issues that have been identified, including steps to minimize further security risks to those individuals whose personal information was lost, compromised, or potentially compromised.

(6) The Contractor shall confer with SSA personnel in reviewing the actions the Contractor has taken and plans to take in dealing with the breach or incident. Additionally, the Contractor shall provide any documentation requested by SSA.

(7) The Contractor shall bear the cost for any data breach or incident: (1) occurring outside of SSA-controlled facilities, systems, or environments when the affected PII was in the possession or control of the Contractor or its employees, agents, or representatives; or (2) resulting from the Contractor or its employees, agents, or representatives' failure to properly safeguard PII or facilities, systems, or other environments containing PII in accordance with this contract's requirements. In addition, as SSA requires, the Contractor shall be responsible for or shall assist SSA in taking preventative and remedial actions that SSA determines are necessary to address such a breach or incident. Preventative and remedial actions may include notification to individuals potentially affected by the breach and other countermeasures to mitigate the risk of harm or to protect PII (e.g., operating call centers and providing resources for potentially affected individuals). SSA will notify the Contractor when SSA determines that preventative or remedial action(s) are necessary and instruct the Contractor on whether the action(s) will be effectuated by the Contractor or SSA. SSA may choose to effectuate the action(s) at the agency's discretion. The Contractor shall be responsible for the cost of all preventative or remedial action(s), including those actions effectuated by SSA, resulting from the breaches and incidents covered by this paragraph. Note: Nothing in this paragraph affects the Contractor's obligations in paragraph (e)(2) above to take immediate steps to address identified security issues.

(f) *Subcontractor(s).*

(8) The Contractor shall include this clause in all resulting subcontracts whenever there is any indication that the subcontractor(s) and their employees, or successor subcontractor(s) and their employees, will or may handle PII. When this clause is included in a subcontract, all references to "Contractor" in paragraphs (a) through (e) and (h) shall be read to apply to the subcontractor(s).

(9) The Contractor shall take appropriate and necessary action to ensure its subcontractor(s) and their employees, or any successor subcontractor(s) and their employees, comply with this clause.

(10) *Notification of Subcontractor Handling of PII.* If the Contractor engages a subcontractor under this contract whose employee(s) will actually or potentially handle PII, the Contractor shall do the following:

(i) Notify the SSA COR and the Contracting Officer of this arrangement in advance of providing access to PII, providing the subcontractor name(s) and address(es) and, upon request, a description of the nature of the PII to which the employee(s) will actually or potentially be given/have access (e.g., phone numbers, SSN); and

(ii) Provide the agency's COR the names of the subcontractor employee(s) who will actually or potentially be assigned and/or have access to the PII. The Contractor may satisfy this requirement when submitting the name(s) of the subcontractor employee(s) to the agency's COR for the requisite security

background check described in paragraph (g), below.

(g) *Security & Suitability Requirements Clause.* For each Contractor employee handling PII, the Contractor shall fulfill the requirements of the Security & Suitability Requirements Clause, found elsewhere in this contract, to ensure that any such individual has the appropriate background checks.

(h) The Contractor shall permit the agency to conduct security reviews and inspections to ensure that the Contractor maintains adequate safeguards and security measures for PII in accordance with the terms of this contract. At SSA's request, the Contractor shall grant SSA, and its auditors, access to all systems, facilities, equipment, locations, and other environments that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII for such reviews and inspections. The Contractor is not required to provide SSA access to parts of those systems, facilities, equipment, locations, and other environments that are not impacted by such reviews and inspections.

(End of clause)

2352.224-2B – Worksheet for Reporting a Loss or a Suspected Loss of Personally Identifiable Information (PII) (MAY 2026)

INSTRUCTIONS

The purpose of this worksheet is to assist individuals, entities (including contractors), or agencies who lose or suspect the loss of Social Security Administration (SSA) PII. (See Note number 1, below.) This worksheet should be used as an information-gathering tool to quickly organize and report to SSA the needed information about the loss or suspected loss. However, **do not include PII specific to the loss on this worksheet**.

Employees and individuals should not wait until confirmation of loss occurred before reporting. Both confirmed and suspected losses should be timely reported. A delay may undermine the agency's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals.

All PII losses, suspected or confirmed, should be reported within one (1) hour of discovery using the online Loss Reporting Tool (LRT) at https://ssaprod.servicenowservices.com/ecsd?id=sc_cat_item_guide&sys_id=8c018b211b3f1e1044dba8eae54bcbcd&sysparm_category=8f24c8f81b50e210025bea42f54bcb7e (see Note number 2, below) or by calling SSA's Enterprise IT Customer Service Desk at 1-877-697-4889 (website address: https://ssaprod.servicenowservices.com/ecsd).

Notes:

1. PII is information that can be used to distinguish or trace an individual's identity, either along or when combined with other information that is linked or linkable to a specific individual (e.g., name, date of birth, Social Security number).

2. The LRT is located on the SSA Intranet and may not be accessible to all contractors.

Basic Information for the Contractor for Reporting PII Loss (Suspected or Confirmed):

a. Your primary agency contact for reporting PII breach incidents. This is: [*Contracting Officer: Fill in the name and contact information (phone number(s), address, etc.) of the primary agency contact. This should be the Contracting Officer's Representative (COR). For task-order contracts with various COR-Task Managers, write, "Also, contact the Task Manager."*]

b. The alternates to this primary contact. They are as follows:

First Alternate: [*Contracting Officer: Fill in the name and contact information (work phone number(s), address, etc.) of the First Alternate agency contact. This should be the Alternate COR.*]

Second Alternate: [*Contracting Officer: Fill in the name and contact information (work phone number(s), address, etc.) of the Second Alternate agency contact. If none, write "N/A."*]

c. The contract number: [*Contracting Officer: Fill in the contract number when available.*]

d. Agency/Entity/Office (see Item #1 of the worksheet): [*Contracting Officer: fill in the office name of the*

program office where the contractor will be working, including the Deputy Commissioner-level office. If the answer can vary, e.g., under a task-order contract where there are a number of offices, you may write "Various" and instruct the COR to have each Task Manager fill in this information and provide the filled-in copy to the contractor for distribution to its employees working under the task order.]

1. **Information about the individual making the report:**

   Name:

   Position:

   Agency/Entity/Office:

   Work Email Address:

   Work Phone Number:

   Date of Report to SSA:

2. **Is the individual, who was in possession of the data or to whom the data was assigned, different from the person making the report (as listed in #1)?**

   Same as person making the report? [ ] Yes [ ] No

   If no, complete the following for the individual who was in possession/assigned the data:

   Name:

   Position:

   Agency/Entity/Office:

   Work Email Address:

   Work Phone Number:

3. **Circumstances of the breach:**

   Is the incident a result of robbery or theft? [ ] Yes [ ] No

   Did the incident include equipment? [ ] Yes [ ] No

   Full description of how the incident occurred:

Date/Time of Incident:

4. **Information about the data that was lost/stolen:**

Describe what was lost or stolen:

Did the incident occur while teleworking or performing duties at (or traveling to/from an alternative worksite?

Estimated number of individuals affected:

What elements of PII did the data contain?

[ ] Name
[ ] Social Security number
[ ] Date of Birth
[ ] Place of Birth
[ ] Address
[ ] Other (describe):
[ ] Bank Account Information
[ ] Medical/Health Information
[ ] Benefit Payment Information
[ ] Mother's Maiden Name
[ ] Medicare Beneficiary Identifier

Are you able to identify the individual(s) whose information was compromised?

[ ] Yes [ ] No

5. **How was the data physically stored, packaged and/or contained? If electronic, check the appropriate response below:**

[ ] Laptop
[ ] Hard Drive
[ ] USB Drive
[ ] Server
[ ] Cell Phone/Black Berry
[ ] Workstation
[ ] CD/DVD
[ ] Tablet
[ ] Cloud
Phone Number:

Hardware Make/Model: Hardware Serial Number:

[ ] Email

[ ] Other (describe):

Was the device encrypted? [ ] Yes [ ] No

Was the device password protected? [ ] Yes [ ] No

Was a VPN SmartCard lost? [ ] Yes [ ] No

6. Others contacted and reports filed about the breach: (Include Deputy Commissioner level, agency level, regional/associate level component names)

Federal Protective Service Report: [ ] Yes [ ] No

Local Police Report: [ ] Yes [ ] No

AIRS Incident Reporting Form: [ ] Yes [ ] No

SSA-342: [ ] Yes [ ] No

Other:

Have other SSA components been contacted? [ ] Yes [ ] No

If so, please list other contacted SSA components (including the OIG):

Media Interest: [ ] Yes [ ] No

Congressional Interest: [ ] Yes [ ] No

Actions Taken:

Other Information:

(End of clause)

Attachment A.2.C - 2352.224-1 Protection of Confidential Information (DEC 2024)

(a) Definitions. As used in this clause—

"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 recipient for, or otherwise obtained by the recipient in, the performance of this grant; and (2) of a personal nature about an individual, such as name, home address, and Social Security number, or 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 (FTI); or information designated by SSA as confidential for other reasons. Confidential information includes all personally identifiable information (PII) provided by SSA or collected or acquired by the recipient as a result of this grant. 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.

“Federal tax information (FTI)” means 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 PII.

“Personally identifiable information (PII)” means 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 Recipient as a result of performing under this grant or provided by SSA.

(b) In addition to what is deemed confidential information in (a) above, the Contracting Officer and the Recipient may, by mutual consent, identify elsewhere in this grant specific information or categories of information that the Government will furnish to the Recipient or that the Recipient is expected to generate which are confidential. Similarly, the Contracting Officer and the Recipient may, by mutual consent, identify such confidential information from time to time during the performance of the grant. All confidential information will be used only for purposes delineated in the grant; any other use of the confidential information will require the Contracting Officer’s express written authorization. The Contracting Officer and the Recipient will settle any disagreements regarding the identification pursuant to the "Disputes" clause.

(c) The Recipient shall restrict access to all confidential information to the minimum number of employees who need it in connection with the performance of work under this grant. Employees who need access to confidential information for performance of the grant will be determined in conference between SSA’s Contracting Officer, Contracting Officer’s Representative, and the responsible Recipient official. Upon request, the Recipient will provide SSA with a list of “authorized employees,” that is, all employees who have or will have access to confidential information covered by this clause.

(d) The Recipient shall process all confidential information under the immediate supervision and control of authorized employees in a manner that will: protect the confidentiality of the records; prevent the unauthorized use of confidential information; and prevent access to the records by unauthorized persons.

(e) The Recipient shall inform all authorized employees of the confidential nature of the information and the administrative, technical and physical safeguards required to protect the information from improper disclosure. All confidential information shall, at all times, be stored in an area that is physically safe from unauthorized access. See paragraph (f) below regarding the minimum standards which the safeguards must meet.

(f) Whenever the Recipient is storing, viewing, transmitting, or otherwise handling confidential information, the Recipient shall comply with the applicable standards for security controls that are established in the Federal Information Security and Management Act (FISMA) and by SSA. (These standards include those set by the National Institute of Standards and Technology (NIST) via the Federal Information Processing Standards (FIPS) publications and NIST Special Publications, particularly FIPS 199, FIPS 200, and NIST Special Publications - 800 series.)

(g) The Recipient's use of confidential information, in the performance of the grant, is subject to the Privacy Act of 1974, 5 U.S.C. § 552a; the Social Security Act, 42 U.S.C. § 1306; and SSA's regulations at 20 C.F.R. Part 401. All such information shall be confidential and shall not be disclosed without the written permission of the Contracting Officer.

(h) The Recipient shall assure that its subrecipient(s) and their employees or any successor subrecipient(s) and their employees with access to confidential information are made aware of the prescribed rules of conduct and criminal penalties for violations of the Privacy Act and the Social Security Act. For knowingly disclosing information in violation of the Privacy Act, the Recipient and Recipient employees may be subject to the criminal penalties as set forth in 5 U.S.C. § 552(i)(1) to the same extent as employees of SSA. The Recipient and Recipient employees may be subject to the criminal penalties for disclosures that are not in accordance with SSA's regulations (20 C.F.R. Part 403). (42 U.S.C. § 1306(a)). For willfully disclosing confidential tax return information in violation of the IRC, the Recipient and Recipient employees may be subject to the criminal penalties set forth in 26 U.S.C. § 7213.

(i) Whenever the Recipient is uncertain how to handle properly any material under the grant, the Recipient must obtain written instructions from the Contracting Officer addressing this question. If the material in question is subject to the Privacy Act or section 1106 of the Social Security Act or is otherwise confidential information subject to the provisions of this clause, the Recipient must obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication. Contracting Officer instructions and determinations will reflect the result of internal coordination with appropriate program and legal officials.

(j) The Government reserves the right to conduct on-site visits to review the Recipient's documentation and in-house procedures for protection of and security arrangements for confidential information and adherence to the terms of this clause.

(k) The Recipient shall include this clause in all resulting subcontracts whenever there is any indication that the subrecipient(s), engaged by the recipient, and their employees or successor subrecipient(s) and their employees might have access to confidential information.

(l) Federal tax information. (1) This grant [x] does [ ] does not entail, or potentially entail, the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of FTI.

(2) If this grant entails FTI, the Recipient shall also comply with the provisions of Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies (Pub. 1075), Exhibit 7, found at https://www.irs.gov/pub/irs-pdf/p1075.pdf, as amended. The Recipient shall adhere to the current version of Pub. 1075. At a minimum, the Recipient shall check on or around the anniversary date of the grant or grant modification providing for this clause, as applicable, for any updates to this exhibit. The provisions of Pub. 1075 Exhibit 7 do not override or amend the Recipient's responsibility set forth in this grant for confidential information. If the Recipient has a question about compliance with grant terms, it shall promptly raise its question to the Contracting Officer.

(End of clause)

ATTACHMENT B- 2352.204-1 – Security and Suitability Requirements-GRANTS (MAY 2026)

(a) Acronyms and Definitions – As used in this clause –

"Access to a facility, site, system, or information" means physical access to any Social Security Administration (SSA) facility or site, logical access to any SSA information system, or access to programmatic or sensitive information.

"GMO" means grants management officer.

"Grant personnel" means employees of the recipient, employees of the subawardee, any consultant retained by the recipient or subawardee, any volunteer or intern of the recipient or subawardee, and if the recipient or subawardee is a sole proprietorship, it refers to the sole proprietorship.

"PO" means program officer

"RPOC" means recipient point of contact as specified by the grant award.

"PerSec" means Personnel Security.

"e-App" means electronic application which contains the investigative Standard Forms (SF) contractor employees use to input information required to process their personnel background investigation

"PIV" means Personal Identity Verification.

"NBIS" means National Background Investigation Services.

(b) Purpose

This clause provides SSA's policies and procedures concerning the conduct of background investigations (i.e. suitability determinations) of recipient personnel. A background investigation is required any time recipient personnel requires any type of access to a SSA facility, site, system, or information, whether or not a PIV credential is required. Recipient personnel may be subject to periodic reinvestigation per SSA policy. The purpose of these investigations is to determine the suitability of recipient personnel needing access to a SSA facility, site, system, or information. If applicable, the clause also describes the process to obtain a PIV credential.

(c) PIV Credentials

(1) A PIV credential is required for recipient personnel requiring access to a SSA information system or routine, unescorted access to a SSA facility or site for a period of six months or more. (See paragraph (k) for more information.)

(2) A PIV credential is not required for:

(i) Recipient personnel requiring escorted access to a SSA facility or site for less than six months; or

(ii) Recipient personnel requiring infrequent escorted access to a SSA facility or site, even if the access may be longer than six months (e.g., recipient personnel who provide infrequent facilities or equipment maintenance or repair, or who conduct onsite shredding, etc.).

(d) Authorities

(1) Homeland Security Presidential Directive 12 (http://www.dhs.gov/homeland-security-presidential-directive-12).

(2) Office of Management and Budget Memorandum M-05-24 (OMB Memorandum M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors | Cyber Security: Executive Orders and Policies).

(3) The Crime Control Act of 1990, Public Law 101-647, subtitle E, as amended by Public Law 102-190 (for childcare center security requirements) (public law 101-647, subtitle E).

(4) Executive Orders 13764 and 12968

(DCPD-201700051 - Executive Order 13764-Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters - Content Details -) and

https://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf)

(5) Title 5, Code of Federal Regulations (CFR), Parts 731, 736, and 1400 (for positions assigned a "National Security" designation) (http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5cfr731_main_02.tpl, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5cfr736_main_02.tpl, and http://www.ecfr.gov/cgi-bin/text-idx?SID=ea8d9b7f129b58c4b512ea9d68a44761&mc=true&node=pt5.3.1400&rgn=div5%23se5.3.1400_1201)

(6) The Fair Chance to Compete for Jobs Act of 2019 (National Defense Authorization Act for Fiscal Year 2020) and the respective Federal regulations (5 CFR Parts 302, 317, 319, 330, 731, 754, and 920). Per the Fair Chance Act, the contractor may not verbally, or through written form, request the disclosure of criminal history record information regarding an applicant for a position related to work under such contract before the contractor extends a conditional offer to the applicant.

(e) Suitability Process

The background investigation and adjudication processes are compliant with 5 CFR 731 or equivalent.

SSA is required to submit fingerprints to the Federal Bureau of Investigation (FBI) as part of the Federal personnel background investigation process. This requirement is per HSPD-12 and is mandatory for everyone within the SSA workforce, including contractor employees.

The FBI maintains fingerprint images and uses these images to report any criminal activity by contractor employees to SSA, specifically any criminal activity that may occur after the completion and adjudication of the required background investigation. The FBI's "Next Generation Information Rap Back program" (Rap Back) requires agencies to enroll contractor employees into this program.

Contractors must notify their contractor employees who work on SSA contracts to carefully review and understand the FBI Privacy Act Statement and the Noncriminal Justice Applicant's Privacy Rights

Statement. These documents contain vital information about individual's rights and how their information will be handled. If SSA records do not contain classifiable fingerprints, PerSec will provide contractor employees with instructions to submit updated fingerprints.

Any contractor employee requiring access to a SSA facility, site, system, or information must complete and submit, through the COR, the documents listed in (d)(1) at least 30 business days prior to the date contractor employees are to begin work. The suitability process cannot begin until the contractor submits, and SSA receives, accurate and complete documents.

(1) Suitability Document Submission

a. Immediately upon award, the RPOC must provide to the PO for all recipient personnel requesting a suitability determination:

(A) A Completed Optional Form (OF) 306, Declaration for Federal Employment;

(B) Proof of citizenship and/or work authorization for non-United States (U.S.) born applicants, if applicable.

(C) An Applicant Listing that must include the recipient's name, the grant award number, the GMO's name, the RPOC's contact information, the PO's name, the PO's contact information, and the full name, Social Security Number, date of birth, place of birth (must show city and state if born in the U.S. OR city and country if born outside of the U.S.), a valid email address for all recipient personnel requesting suitability, and the date the recipient completed fingerprinting. All spelling of names, email addresses, places, and numbers must be accurate and legible.

(D) The required suitability forms, and a sample of properly completed forms, are available on SSA's Strategic Sourcing website at [https://www.ssa.gov/oag/acq/ASC_2352_204-1_Security_and_Suit_Reqrmts_Post_10012017/Links%20for%20Agency%20Specific%20Clause%202352_204-1%20Post%2010012017.htm]).

Commented [SN1]: Broken Link: https://www.ssa.gov/oag/acq/oagacq_security.htm new link

Commented [SN2R1]: Agency Specific Clause 2352.204-1, Security and Suitability Requirements March 2018

(2) eApp Form and Fingerprint Submission

(i) Once SSA receives all completed documents, listed in (d)(1), PerSec will initiate the suitability screening process in eApp using the Applicant Listing. PerSec will email the eApp notification to the GMO and PO inviting recipient personnelto electronically complete the background investigation form (Standard Form SF 85P, Questionnaire for Public Trust Positions.. Recipient personnel will receive one account creation email from noreply@nbis.mil. The subject line will read *Action Required* Activate Your New NBIS eApp Account. The email will prompt recipient employees to set up a password code.

i. Recipient personnel will have 5 business days to complete their investigative form. The 5-day timeframe begins the day PerSec sends the invitation to the GMO and PO. Recipient personnel must electronically sign the signature pages before releasing the application in eApp. After form submission, recipient personnel can download copies of their form and relevant documents. Please note, reviewing the form prior to submission can only be done in eApp. The SF85P does not become available for download until it has been submitted in eApp.

(iii). Information about the eApp process is available on the NBIS website

a. (A) Recipient personnel must schedule and complete fingerprinting prior to the initial submission. The PO and RPOC will be given the fingerprint instructions.

(3) Status Check

If contractor employees have completed each of the steps in (d)(1) and (2) in their entirety and do not receive a suitability determination within 15 business days of their last submission, email SecRes.PerSec.Contractor.Vetting@ssa.gov or contact the designated PerSec point of contact.

(f) Suitability Determination

(1) PerSec uses an FBI fingerprint check as part of the basis for making a preliminary suitability determination. This determination is final unless information obtained during the remainder of the full background investigation, conducted by SSA's Investigative Service Provider, is such that SSA would find the recipient personnel unsuitable to continue performing under this award. PerSec will notify the RPOC and the PO of any unsuitable determinations.

(2) SSA will not allow recipient personnel access to a facility, site, information, or system until PerSec issues a favorable preliminary suitability determination. A favorable preliminary suitability determination letter, issued by PerSec, is valid only for performance on the award specified in the letter.

(3) If current recipient personnel are to perform work under a new award, the RPOC must submit a fully completed, legible Recipient Personnel Rollover Request Form to the PO of the new award. PerSec will notify the RPOC and the PO of suitability to work on the new award. The Recipient Personnel Rollover Request Form is on Strategic Sourcing' website.

(g) Recipient Personnel Previously Cleared by SSA or Another Federal Agency

If recipient personnel previously received a suitability determination from SSA or another Federal agency, the previous investigation will be reviewed to determine transfer of trust. If transfer of trust applies, there will be no eApp initiated and PerSec will issue the favorable determination letter with our any additional steps needed from the personnel.

(h) A recipient is not entitled to an equitable adjustment of the award because of an unfavorable suitability determination(s). Additionally, if SSA determines that the number or percentage of unfavorable determinations make successful award performance unlikely, SSA may terminate the award for cause or default.

(i) Unsuitable Determinations

(1) The recipient must notify the recipient personnel of any unsuitable determinations as soon as possible after receipt of such a determination.

(2) The recipient must submit requests for clarification for unsuitable determinations in writing within 30 days of the date of the unsuitable determination to the email mailbox or address listed below. Recipient personnel must file their own requests; recipients may not file requests on behalf of recipient personnel.

SecRes.PerSec.SuitClarify@ssa.gov OR

Social Security Administration

Center for Suitability and Personnel Security

Attn: Suitability Program Officer

6401 Security Boulevard

2246 Annex Building

Baltimore, MD 21235

(3) There is no appeals process for recipient personnel unsuitable determinations.

(j) Continuous Vetting (CV)

Executive Order 13764 directed reforms of the Executive Branch personnel vetting program, including mandating the use of CV for anyone working for or on behalf of the Government. CV requires regular reviewing an individual's background to ensure they continue to meet suitability requirements. This includes periodically obtaining updated background investigation forms from contractor employees.

(k) Recipient Notification to Government

The recipient shall notify the PO and PerSec within one business day if any recipient personnel is arrested or charged with a crime during the term of this award, or if there is any other change in the status of recipient personnel (e.g. leaves the company, no longer works under the grant award, the alien status changes, etc.) that could affect their suitability determination. The recipient must provide in the notification as much detail as possible, including, but not limited to: name(s) of recipient personnel whose status has changed, award number, the type of charge(s), if applicable, date of arrest, the court date, jurisdiction, and, if available, the disposition of the charge(s).

(l) Obtaining a Credential

(1) This section applies only if recipient personnel will have access to a SSA information system or routine or unescorted access to a SSA facility or site for a period of six months or more as described in paragraph (c)(1).

(2) Once the recipient personnel receive notification of an acceptable suitability determination, but prior to beginning work under the award, the recipient personnel must appear at the respective Regional Security Office or SSA Headquarters Parking and Credentialing Office to begin the credentialing process.

(3) The recipient must contact the PO to arrange for credentialing.

(4) Once the PO makes the appointment, the PO must contact the recipient to inform the recipient of the credentialing appointment(s). The PO will also arrange for the recipient personnel to be escorted (by either the PO or a program office's representative) to the appropriate credentialing office at the time of this appointment.

(5) The recipient personnel must present the suitability determination letter and two forms of identification at this meeting. At least one of the forms of identification must be a Government-

issued photo identification (ID) (for acceptable forms of ID see List of Acceptable Documents on Strategic Sourcing's website). A signed and dated SSA-222 is also a required document (see agency specific clause 2352.204-2, Federal Information Security Modernization Act and Agency Privacy Management on Strategic Sourcing's website). For SSA Headquarters access, a completed Form SSA-4395, Application for Access to SSA Facilities, signed by the recipient personnel and the PO is also required. The PO will provide the SSA-4395 Form to the recipient personnel when applicable.

(6) Credentialing appointments last approximately 15 minutes. Depending on a recipient's scheduling needs and availabilities, recipient personnel may be scheduled for credentialing all in one day (this process may take a few hours to complete, depending on the number of recipient personnel that need to be credentialed) or they may come in at separate times convenient to the recipient personnel's and the PO's schedules.

(7) Contacts

a. SSA Headquarters' Parking and Credentialing Office representatives can be reached at Parking.and.Credentialing@ssa.gov or 410-965-5910.

(i) Contact information for other SSA facilities is available on Strategic Sourcing's website, in the *Security and Suitability Business Process Guide*.

b. Regional Security Office contact information is in the Appendix at the end of this clause.

(m) Recipient Return of PIV Credential

The recipient must account for and ensure that all forms of Government-provided identification (PIV credential) issued to recipient personnel under this award are returned to SSA's Headquarters' Parking and Credentialing Office or Regional Security Office, as appropriate, as soon as any of the following occur: when no longer needed for award performance; upon completion of any recipient personnel employment; or upon award completion or termination.

(n) Government Control

The Government has full control over and may grant, deny, or withhold access to a facility, site, system, or information and may remove recipient personnel, or require the recipient to remove recipient personnel from performing under the award for reasons related to conduct even after recipient personnel are found suitable to work on the award (see paragraph (n) below).

(o) Removal From Duty

The GMO, in coordination with the PO and PerSec, may remove a recipient personnel, or request the recipient immediately remove any recipient personnel from working under the award based on conduct that occurs after a favorable suitability determination. This includes temporarily removing recipient personnel arrested for a violation of law pending the outcome of any judicial proceedings. The recipient must comply with these requests to remove any recipient personnel. The Government's determination may be made based on, but not limited to, these incidents involving the misconduct or delinquency:

(1) Violation of the Rules and Regulations Governing Public Buildings and Grounds, 41 CFR 101-20.3. This includes any local credentialing requirements.

(2) Neglect of duty, including sleeping while on duty; unreasonable delays or failure to carry out assigned tasks; conducting personal affairs while on duty; and refusing to cooperate in upholding the integrity of SSA's security program.

(3) Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents, records, or Government property or concealment of material facts by willful omissions from official documents or records.

(4) Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting. Also, participating in disruptive activities that interfere with the normal and efficient operations of the Government.

(5) Theft, vandalism, or any other criminal actions.

(6) Selling, consuming, possessing, or being under the influence of intoxicants, drugs, or substances that produce similar effects.

(7) Improper use of official authority or credentials.

(8) Unauthorized use of communications equipment or Government property.

(9) Misuse of weapon(s) or tools used in the performance of the award.

(10) Unauthorized access to areas not required for the performance of the award.

(11) Unauthorized access to SSA’s employees' personal property.

(12) Violation of security procedures or regulations.

(13) Prior recipient personnel unsuitability determination by SSA or another Federal agency.

(14) Unauthorized access to, or disclosure of, agency programmatic or sensitive information, or Internal Revenue Service Tax Return information.

(15) Failure to ensure the confidentiality of or failure to protect from disclosure, agency information entrusted to them. Certain provisions of these statutes and regulations apply to Federal employees and apply equally to recipient personnel: The Privacy Act of 1974, The Tax Reform Act of 1976 and the Taxpayer Browsing Protection Act of 1997, SSA regulation 1, The Computer Fraud and Abuse Act of 1986, and Section 1106 of the Social Security Act.

(16) Being under investigation by an appropriate authority for violating any of the above.

(p) The recipient is required to include the substance of this clause in any subaward requiring the subrecipient to access a SSA facility, site, system, or information. However, the recipient must obtain, review, and submit to SSA all of the completed and required forms (see paragraph (e) from the subawardee. SSA will not accept completed forms from anyone other than the recipient.

Appendix:

Regional Security Offices

Regional Credentialing Contacts for Grant Personnel

Northeast Region

For the following states and territories: CT, DC, DE, MA, MD, ME, NH, NJ, NY, PA, PR, RI, VA, VI, VT, WV

NE.ARC.MOS@ssa.gov

Mid-West/West Region

For credentialing within 50 miles of City of Chicago:

CHI.ARC.MOS@ssa.gov

For the following states: AK, CO, IA, ID, IL, IN, KS, MI, MN, MO, MT, ND, NE, OH, OR, SD, UT, WA, WI, WY

||MWW ARC MOS

Southeast Region

For the following states: AL, FL, GA, KY, MS, NC, SC, TN

||ATL MOS ATL.MOS@ssa.gov

Southwest Region

For the following states: AR, LA, NM, OK, TX

||DA ARC MOS DA.ARC.MOS@ssa.gov

For California: SF.ARC.MOS@ssa.gov

For credentialing within 50 miles of City of San Francisco:

^SF CA RO CMR HBFT Help Desk

For the following states and territories: AS, AZ, HI, GU, NV

SW.ARC.MOS@ssa.gov

(End of clause)

Attachment C - DATA PROTECTION, PRIVACY, AND SECURITY REQUIREMENTS

The awardee must comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a); related Office of Management and Budget guidelines; the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283) (collectively, FISMA); and related National Institute of Standards and Technology (NIST) guidelines, as well as any amendments published after the effective date of the award.

SSA will provide the awardee with an SSA-imaged workstation, conduct a suitability background check, issue a Personal Identity Verification (PIV) Card, and establish a Virtual Private Network (VPN) account.

The awardee must comply with the following security requirements:

1. All processing, storage, and transmittal of confidential information must utilize the SSA-provided device and related VPN account, unless expressly authorized in this award or in writing by SSA.
2. Access to, manipulation of, and transmittal of confidential information must use an SSA-provided device, login via the PIV Card, and use of VPN account.
3. Confidential information must not be stored or maintained on non-SSA-provided devices, software, or equipment.
4. The awardee (and subrecipients) working under this grant who will have access to any kind of confidential information as referenced herein, must receive periodic training in computer security awareness and accepted computer security practice.
5. All work performed outside of a grantee's official place of work that is in the grantee's established business office in a commercial setting must be done in accordance with SSA's SPSSBA telework policy. The agency may and will promulgate and revise the SPSSBA telework policy at any time.

The awardee must comply with the following data protection, privacy, and security-related requirements:

(1) Safe Handling Requirements

The awardee must enforce the following information handling requirements for all confidential information:

a. Limit access to confidential information only to persons satisfying personnel suitability determination requirements as prescribed in the suitability section of the award and who have received positive suitability determinations from SSA.

b. Restrict access to confidential information to the minimum number of individuals who need to perform work under the award.

c. Process confidential information under the supervision of authorized personnel (i.e., manager who has received a positive SSA suitability determination and is familiar with proper handling requirements identified herein).

d. Inform all personnel with access to confidential information of the nature of the information and required safeguards to protect it.

e. Flow down the same safe handling requirements and all other privacy and security and records-related requirements in the award to any subrecipients that handle confidential information.

f. Explain to employees that they are responsible for protecting confidential information at all times, both on and off duty. Only permit employees to access the information they need to perform work under this award and disclose such information when authorized under this award.

g. Train employees to handle confidential information responsibly and remind them periodically of their responsibilities.

h. Train managers to recognize situations where employees have failed to adequately safeguard confidential information by failing to secure it from theft, loss, or accidental disclosure. If theft, loss, or accidental disclosure of PII occurs, document in accordance with Attachment A.2.A: 2352.224-2A - Protecting and Reporting the Loss of Personally Identifiable Information: Responsibilities Concerning Individual Employees (June 2023) incorporated into this award.

(2) Transporting Confidential Information Outside a Secure Area/Secure Duty Station:

a. The awardee must ensure that confidential information must remain within in the United States, its territories or possessions, unless authorized by SSA.

b. When transporting confidential information, the awardee must secure and lock the materials in a locked trunk, briefcase, or other lockable device during transport. The awardee must ensure that this information is not left in the passenger compartment of any vehicle.

c. After the employee reaches his/her intended destination, the employee must ensure that he/she does not leave confidential information in the vehicle but securely stores them at the destination in in a locking device such as a briefcase, safe, or other locked container.

d. The awardee must ensure that confidential information, including electronic devices with such information on them, are not left out of the individual's control while transporting them (this requirement may be subject to Transportation Security Administration regulations when traveling by air).

e. The awardee must educate employees, grantees, and subrecipients about which confidential information records can be taken off site and when they can be taken off site. This includes any records and information on laptop computers or other electronic devices as well as paper files.

f. The awardee must have a system that tracks any confidential information records taken off site (for example, if an employee must take work home) to ensure their timely return to the office.

(3) Preventing Identity Theft:

The awardee must:

a. Avoid leaving paper documents and records containing confidential information unprotected.

b. Follow records transfer procedures in Section (6) below.

c. If SSA authorizes awardee to use either the Government Services Online (GSO) or an SSA provided VPN to securely transmit or receive confidential information, awardee employees needing access to GSO must register with GSO and obtain user accounts. Should the awardee be unable to transmit data using GSO or an SSA-provided VPN, the awardee must contact SSA to seek an authorized means of transmitting or receiving confidential information.

d. Ensure that all devices used to transmit, store, process, and receive confidential information are protected to ensure the security of such information. All systems/devices must be password protected and have two-factor authentication. Awardee must only use software and platforms approved by SSA to transmit, store, process, and receive confidential information. No confidential information shall be stored or processed on removable media.

e. Lock or log off the computer when leaving it unattended.

(4) SSA prescribed standards or policies on encryption and password protection of portable electronics devices and removable media containing confidential information: Confidential information on mobile computers/devices and removable media must be encrypted, using an encryption solution that complies with Federal Information Processing Standards (PIPS) 140-2. See link to publication: http://csrc.nist.gov/groups/STM/cmvp/standards.html.

Additionally, the awardee must comply with the following requirements:

a. Encryption-related information (such as keys) must be secured when unattended or not in use.
b. Knowingly decrypting confidential information, the awardee is unauthorized to view is strictly prohibited.

(5) Confidentiality and files:

a. The awardee must protect confidential information from unauthorized access, use, disclosure, and dissemination at all times, whether at-rest or in transit.

b. Disclosure of confidential information that constitutes PII must be consistent with the Privacy Act of 1974 and SSA's privacy regulations, 20 C.F.R. Part 401.

c. The awardee will access, use, and disclose confidential information only for the purpose of performing work for SSA under the term of this award and as otherwise authorized in this award. Unless expressly authorized in this award, the awardee must not disclose confidential information to any person or entity other than SSA without SSA's written permission.

d. The awardee will not access, use, or disclose confidential information, except as necessary to provide services to SSA.

e. If the awardee receives a request, subpoena, or court order for confidential information, the awardee will promptly provide the agency notice of such request. The awardee will provide the agency with the information or tools required for the agency to respond to the request. The awardee may refer the requester to the agency. The awardee will comply with 20 C.F.R. Part 403 and not provide the requester any confidential information unless authorized by the agency.

f. Only awardee employees (or subrecipients, or grantees, when applicable) that have received a favorable suitability determination from SSA may view confidential information.

g. The awardee must provide privacy notices as directed by SSA as part of information collections performed under this award.

(6) Upon the expiration or termination of this award, the agency must have access to all materials embodying confidential information (in any form and including, without limitation, all summaries, copies, excerpts, and metadata of confidential information) at no additional cost to the agency. The awardee must promptly transfer all confidential information back to SSA. No copies of confidential information are authorized to be retained by

awardee.

(7) For any issues/questions regarding privacy, retention, destruction, or systems and security requirements, the awardee should contact SSA immediately for clarification, guidance, or for further discussion.

(8) SSA retains the right to conduct security reviews and onsite inspections of all facilities and locations at which the awardee maintains confidential information to ensure that the awardee maintains adequate safeguards and security measures in accordance with the terms of this award.

(9) In accordance with Office of Management and Budget (OMB) Memorandum 17-12 (M-17-12), the awardee must comply with the following terms:

- Exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach of PII;
- Ensure that regular training for grantees and subgrantees is conducted regarding how to identify and report a breach of PII;
- Report to SSA any suspected or confirmed breach of PII [see Attachment A.2] in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay;
- Maintain capabilities to determine what confidential information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access confidential information, and identify the initial attack vector; and
- Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with OMB M-17-12, the agency's breach response plan, and to assist with responding to a breach of PII.

(10) The awardee must allow SSA the ability to immediately access, search, locate, collect, preserve, and process confidential information to comply with requirements under the provisions of the Freedom of Information Act (FOIA) (5 U.S.C. § 552), the Privacy Act (5 U.S.C. § 552a), or as other Federal laws, regulations, or directive require.

(End of Clause)

Attachment D- 48 C.F.R. § 52.245-1 - GOVERNMENT PROPERTY – GRANTS (SEP 2021)

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

Cannibalize means to remove parts from Government property for use or for installation on other Government property.

Grantee-acquired property means property acquired, fabricated, or otherwise provided by the Grantee for performing a grant, and to which the Government has title.

Grantee inventory means-

(1) Any property acquired by and in the possession of a Grantee or subgrantee under a grant for which title is vested in the Government and which exceeds the amounts needed to complete full performance under the entire grant;

(2) Any property that the Government is obligated or has the option to take over under any type of grant, e.g., as a result either of any changes in the specifications or plans thereunder or of the termination of the grant (or subaward thereunder), before completion of the work, for the convenience or at the option of the Government; and

(3) Government-furnished property that exceeds the amounts needed to complete full performance under the entire grant.

Grantee's managerial personnel means the Grantee's directors, officers, managers, superintendents, or equivalent representatives who have supervision or direction of-

(1) All or substantially all of the Grantee's business;

(2) All or substantially all of the Grantee's operation at any one plant or separate location; or

(3) A separate and complete major industrial operation.

Demilitarization means rendering a product unusable for, and not restorable to, the purpose for which it was designed or is customarily used.

Discrepancies incident to shipment means any differences (e.g., count or condition) between the items documented to have been shipped and items actually received.

Equipment means a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for the performance of a grant. Equipment is not intended for sale, and does not ordinarily lose its identity or become a component part of another article when put into use. Equipment does not include material, real property, special test equipment or special tooling.

Government-furnished property means property in the possession of, or directly acquired by, the Government and subsequently furnished to the Grantee for performance of a grant. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes grantee-acquired property if the grantee-acquired property is a deliverable under a cost grant when accepted by the Government for continued use under the grant.

Government property means all property owned or leased by the Government. Government property includes both Government- furnished and Grantee-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property and software.

Loss of Government property means unintended, unforeseen or accidental loss, damage or destruction to Government property that reduces the Government's expected economic benefits of the property. Loss of Government property does not include purposeful destructive testing, obsolescence, normal wear and tear or manufacturing defects. Loss of Government property includes, but is not limited to-

(1) Items that cannot be found after a reasonable search;

(2) Theft;

(3) Damage resulting in unexpected harm to property requiring repair to restore the item to usable condition; or

(4) Destruction resulting from incidents that render the item useless for its intended purpose or beyond economical repair.

Material means property that may be consumed or expended during the performance of a grant, component parts of a higher assembly, or items that lose their individual identity through incorporation into an end item. Material does not include equipment, special tooling, special test equipment or real property.

Nonseverable means property that cannot be removed after construction or installation without substantial loss of value or damage to the installed property or to the premises where installed.

Precious metals means silver, gold, platinum, palladium, iridium, osmium, rhodium, and ruthenium.

Production scrap means unusable material resulting from production, engineering, operations and maintenance, repair, and research and development grant activities. Production scrap may have value when re-melted or reprocessed, e.g., textile and metal clippings, borings, and faulty castings and forgings.

Property means all tangible property, both real and personal.

Property Administrator means an authorized representative of the Granting Officer appointed in accordance with agency procedures, responsible for administering the grant requirements and obligations relating to Government property in the possession of a Grantee.

Property records means the records created and maintained by the grantee in support of its stewardship responsibilities for the management of Government property.

Provide means to furnish, as in Government-furnished property, or to acquire, as in grantee-acquired property.

Real property See Federal Management Regulation 102-71.20 (41 CFR 102-71.20).

Sensitive property means property potentially dangerous to the public safety or security if stolen, lost, or misplaced, or that shall be subject to exceptional physical security, protection, control, and accountability. Examples include weapons, ammunition, explosives, controlled substances, radioactive materials, hazardous materials or wastes, or precious metals.

Unit acquisition cost means-

(1) For Government-furnished property, the dollar value assigned by the Government and identified in the grant; and

(2) For grantee-acquired property, the cost derived from the Grantee's records that reflect consistently applied generally accepted accounting principles.

(b) *Property management.*

(1) The Grantee shall have a system of internal controls to manage (control, use, preserve, protect, repair, and maintain) Government property in its possession. The system shall be adequate to satisfy the requirements of this clause. In doing so, the Grantee shall initiate and maintain the processes, systems, procedures, records, and methodologies necessary for effective and efficient control of Government property. The Grantee shall disclose any significant changes to its property management system to the Property Administrator prior to implementation of the changes. The Grantee may employ customary commercial practices, voluntary consensus standards, or industry-leading practices and standards that provide effective and efficient Government property management that are necessary and appropriate for the performance of this grant (except where inconsistent with law or regulation).

(2) The Grantee's responsibility extends from the initial acquisition and receipt of property, through stewardship, custody, and use until formally relieved of responsibility by authorized means, including delivery, consumption, expending, sale (as surplus property), or other disposition, or via a completed investigation, evaluation, and final determination for lost property. This requirement applies to all Government property under the Grantee's accountability, stewardship, possession or control, including its vendors or subgrantees (see paragraph (f)(1)(v) of this clause).

(3) The Grantee shall include the requirements of this clause in all subawards under which Government property is acquired or furnished for subaward performance.

(4) The Grantee shall establish and maintain procedures necessary to assess its property management system effectiveness and shall perform periodic internal reviews, surveillances, self assessments, or audits. Significant findings or results of such reviews and audits pertaining to Government property shall be made available to the Property Administrator.

(c) *Use of Government property.*

(1) The Grantee shall use Government property, either furnished or acquired under this grant, only for performing this grant, unless otherwise provided for in this grant or approved by the Granting Officer.

(2) Modifications or alterations of Government property are prohibited, unless they are-

(i) Reasonable and necessary due to the scope of work under this grant or its terms and conditions;

(ii) Required for normal maintenance; or

(iii) Otherwise authorized by the Granting Officer.

(3) The Grantee shall not cannibalize Government property unless otherwise provided for in this grant or approved by the Granting Officer.

(d) *Government-furnished property.*

(1) The Government shall deliver to the Grantee the Government-furnished property described in this grant. The Government shall furnish related data and information needed for the intended use of the property. The warranties of suitability of use and timely delivery of Government-furnished property do not apply to property acquired or fabricated by the Grantee as grantee-acquired property and subsequently transferred to another grant with this Grantee.

(2) The delivery and/or performance dates specified in this grant are based upon the expectation that the Government-furnished property will be suitable for grant performance and will be delivered to the Grantee by the dates stated in the grant.

(i) If the property is not delivered to the Grantee by the dates stated in the grant, the Granting Officer shall, upon the Grantee's timely written request, consider an equitable adjustment to the grant.

(ii) In the event property is received by the Grantee, or for Government-furnished property after receipt and installation, in a condition not suitable for its intended use, the Granting Officer shall, upon the Grantee's timely written request, advise the Grantee on a course of action to remedy the problem. Such action may include repairing, replacing, modifying, returning, or otherwise disposing of the property at the Government's expense. Upon completion of the required action(s), the Granting Officer shall consider an equitable adjustment to the grant (see also paragraph (f)(1)(ii)(A) of this clause).

(iii) The Government may, at its option, furnish property in an "as-is" condition. The Grantee will be given the opportunity to inspect such property prior to the property being provided. In such cases, the Government makes no warranty with respect to the serviceability and/or suitability of the property for grant performance. Any repairs, replacement, and/or refurbishment shall be at the Grantee's expense.

(3) The Granting Officer may by written notice, at any time-

(i) Increase or decrease the amount of Government-furnished property under this grant;

(ii) Substitute other Government-furnished property for the property previously furnished, to be furnished, or to be acquired by the Grantee for the Government under this grant; or

(iii) Withdraw authority to use property.

(iv) Upon completion of any action(s) under paragraph (d)(3)(i) of this clause, and the Grantee's timely written request, the Granting Officer shall consider an equitable adjustment to the grant.

(e) *Title to Government property.*

(1) All Government-furnished property and all property acquired by the Grantee, title to which vests in the Government under this paragraph (collectively referred to as "Government property"), is subject to the provisions of this clause. The Government shall retain title to all Government-furnished property. Title to Government property shall not be affected by its incorporation into or attachment to any property not owned by the Government, nor shall Government property become a fixture or lose its identity as personal property by being attached to any real property.

(2) Title vests in the Government for all property acquired or fabricated by the Grantee in accordance with the financing provisions or other specific requirements for passage of title in the grant. Under fixed price type grants, in the absence of financing provisions or other specific requirements for passage of title in the grant, the Grantee retains title to all property acquired by the Grantee for use on the grant, except for property identified as a deliverable end item. If a deliverable item is to be retained by the Grantee for use after inspection and acceptance by the Government, it shall be made accountable to the grant through a grant modification listing the item as Government-furnished property.

(3) *Title under Cost-Reimbursement or Time-and-Material Grants or Cost-Reimbursable line items under Fixed-Price grants*.

(i) Title to all property purchased by the Grantee for which the Grantee is entitled to be reimbursed as a direct item of cost under this grant shall pass to and vest in the Government upon the vendor's delivery of such property.

(ii) Title to all other property, the cost of which is reimbursable to the Grantee, shall pass to and vest in the Government upon-

(A) Issuance of the property for use in grant performance;

(B) Commencement of processing of the property for use in grant performance; or

(C) Reimbursement of the cost of the property by the Government, whichever occurs first.

(f) *Grantee plans and systems*.

(1) Grantees shall establish and implement property management plans, systems, and procedures at the grant, program, site or entity level to enable the following outcomes:

(i) *Acquisition of Property.* The Grantee shall document that all property was acquired consistent with its engineering, production planning, and property control operations.

(ii) *Receipt of Government Property*. The Grantee shall receive Government property and document the receipt, record the information necessary to meet the record requirements of paragraph (f)(1)(iii)(A)(*1*) through (*5*) of this clause, identify as Government owned in a manner appropriate to the type of property (*e.g.*, stamp, tag, mark, or other identification), and manage any discrepancies incident to shipment.

(A) *Government-furnished property*. The Grantee shall furnish a written statement to the Property Administrator containing all relevant facts, such as cause or condition and a recommended course(s) of action, if overages, shortages, or damages and/or other discrepancies are discovered upon receipt of Government-furnished property.

(B) *Grantee-acquired property*. The Grantee shall take all actions necessary to adjust for overages, shortages, damage and/or other discrepancies discovered upon receipt, in shipment of Grantee-acquired property from a vendor or supplier, so as to ensure the proper allocability and allowability of associated costs.

(iii) *Records of Government property.* The Grantee shall create and maintain records of all Government property accountable to the grant, including Government-furnished and Grantee-acquired property.

(A) Property records shall enable a complete, current, auditable record of all transactions and shall, unless otherwise approved by the Property Administrator, contain the following:

(1) The name, part number and description, National Stock Number (if needed for additional item identification tracking and/or disposition), and other data elements as necessary and required in accordance with the terms and conditions of the grant.

(2) Quantity received (or fabricated), issued, and balance-on-hand.

(3) Unit acquisition cost.

(4) Unique-item identifier or equivalent (if available and necessary for individual item tracking).

(5) Unit of measure.

(6) Accountable grant number or equivalent code designation.

(7) Location.

(8) Disposition.

(9) Posting reference and date of transaction.

(10) Date placed in service (if required in accordance with the terms and conditions of the grant).

(B) *Use of a Receipt and Issue System for Government Material*. When approved by the Property Administrator, the Grantee may maintain, in lieu of formal property records, a file of appropriately cross-referenced documents evidencing receipt, issue, and use of material that is issued for immediate consumption.

(iv) *Physical inventory*. The Grantee shall periodically perform, record, and disclose physical inventory results. A final physical inventory shall be performed upon grant completion or termination. The Property Administrator may waive this final inventory requirement, depending on the circumstances (*e.g.*, overall reliability of the Grantee's system or the property is to be transferred to a follow-on grant).

(v) *Subgrantee control*.

(A) The Grantee shall award subawards that clearly identify items to be provided and the extent of any restrictions or limitations on their use. The Grantee shall ensure appropriate flow down of grant terms and conditions (*e.g.*, extent of liability for loss of Government property.

(B) The Grantee shall assure its subawards are properly administered and reviews are periodically performed to determine the adequacy of the subgrantee's property management system.

(vi) *Reports*. The Grantee shall have a process to create and provide reports of discrepancies, loss of Government property, physical inventory results, audits and self-assessments, corrective actions, and other property-related reports as directed by the Granting Officer.

(vii) *Relief of stewardship responsibility and liability*. The Grantee shall have a process to enable the prompt recognition, investigation, disclosure and reporting of loss of Government property, including losses that occur at subgrantee or alternate site locations.

(A) This process shall include the corrective actions necessary to prevent recurrence.

(B) Unless otherwise directed by the Property Administrator, the Grantee shall investigate and report to the Government all incidents of property loss as soon as the facts become known. Such reports shall, at a minimum, contain the following information:

(1) Date of incident (if known).

(2) The data elements required under (f)(1)(iii)(A).

(3) Quantity.

(4) Accountable grant number.

(5) A statement indicating current or future need.

(6) Unit acquisition cost*, or if applicable, estimated sales proceeds, estimated repair or replacement costs.*

(7) All known interests in commingled material *of which includes Government* material*.*

(8) Cause and corrective action taken or to be taken to prevent recurrence.

(9) A statement that the Government will receive compensation covering the loss of Government property*, in the event the Grantee was or will be reimbursed or compensated.*

(10) Copies of all supporting documentation.

(11) Last known location.

(12) A statement that the property *did or did not contain sensitive, export controlled, hazardous, or toxic* material*, and that the appropriate agencies and authorities were notified.*

(C) Unless the grant provides otherwise, the Grantee shall be relieved of stewardship responsibility and liability for property when-

(1) Such property *is consumed or expended, reasonably and properly, or otherwise accounted for, in the performance of the grant, including reasonable inventory adjustments of* material *as determined by the* Property Administrator*;*

(2) Property Administrator *grants relief of responsibility and liability for* loss of Government property*;*

(3) Property *is delivered or shipped from the Grantee's plant, under Government instructions, except when* shipment *is to a subgrantee or other location of the Grantee; or*

(4) Property *is disposed of in accordance with paragraphs (j) and (k) of this clause.*

(viii) *Utilizing Government property*.

(A) The Grantee shall utilize, consume, move, and store Government Property only as authorized under this grant. The Grantee shall promptly disclose and report Government property in its possession that is excess to grant performance.

(B) Unless otherwise authorized in this grant or by the Property Administrator the Grantee shall not commingle Government material with material not owned by the Government.

(ix) *Maintenance*. The Grantee shall properly maintain Government property. The Grantee's maintenance program shall enable the identification, disclosure, and performance of normal and routine preventative maintenance and repair. The Grantee shall disclose and report to the Property Administrator the need for replacement and/or capital rehabilitation.

(x) *Property closeout*. The Grantee shall promptly perform and report to the Property Administrator grant property closeout, to include reporting, investigating and securing closure of all loss of Government property cases; physically inventorying all property upon termination or completion of this grant; and disposing of items at the time they are determined to be excess to grant needs.

(2) The Grantee shall establish and maintain Government accounting source data, as may be required by this grant, particularly in the areas of recognition of acquisitions, loss of Government property, and disposition of material and equipment.

(g) *Systems analysis*.

(1) The Government shall have access to the Grantee's premises and all Government property, at reasonable times, for the purposes of reviewing, inspecting and evaluating the Grantee's property management plan(s), systems, procedures, records, and supporting documentation that pertains to Government property. This access includes all site locations and, with the Grantee's consent, all subgrantee premises.

(2) Records of Government property shall be readily available to authorized Government personnel and shall be appropriately safeguarded.

(3) Should it be determined by the Government that the Grantee's (or subgrantee's) property management practices are inadequate or not acceptable for the effective management and control of Government property under this grant, or present an undue risk to the Government, the Grantee shall prepare a corrective action plan when requested by the Property Administrator and take all necessary corrective actions as specified by the schedule within the corrective action plan.

(h) *Grantee Liability for Government Property*.

(1) Unless otherwise provided for in the grant, the Grantee shall not be liable for loss of Government property furnished or acquired under this grant, except when any one of the following applies-

(i) The risk is covered by insurance, or the Grantee is otherwise reimbursed (to the extent of such insurance or reimbursement). The allowability of insurance costs shall be determined in accordance with 31.205-19.

(ii) Loss of Government property that is the result of willful misconduct or lack of good faith on the part of the Grantee's managerial personnel.

(iii) The Granting Officer has, in writing, revoked the Government's assumption of risk for loss of Government property due to a determination under paragraph (g) of this clause that the Grantee's property management practices are inadequate, and/or present an undue risk to the Government, and the Grantee failed to take timely corrective action. If the Grantee can establish by

clear and convincing evidence that the loss of Government property occurred while the Grantee had adequate property management practices or the loss did not result from the Grantee's failure to maintain adequate property management practices, the Grantee shall not be held liable.

(2) The Grantee shall take all reasonable actions necessary to protect the property from further loss. The Grantee shall separate the damaged and undamaged property, place all the affected property in the best possible order, and take such other action as the Property Administrator directs.

(3) The Grantee shall do nothing to prejudice the Government's rights to recover against third parties for any loss of Government property.

(4) The Grantee shall reimburse the Government for loss of Government property, to the extent that the Grantee is financially liable for such loss, as directed by the Granting Officer.

(5) Upon the request of the Granting Officer, the Grantee shall, at the Government's expense, furnish to the Government all reasonable assistance and cooperation, including the prosecution of suit and the execution of instruments of assignment in favor of the Government in obtaining recovery.

(i) *Equitable adjustment*. Equitable adjustments under this clause shall be made in accordance with the procedures of the Changes clause. However, the Government shall not be liable for breach of grant for the following:

(1) Any delay in delivery of Government-furnished property.

(2) Delivery of Government-furnished property in a condition not suitable for its intended use.

(3) An increase, decrease, or substitution of Government-furnished property.

(4) Failure to repair or replace Government property for which the Government is responsible.

(j) *Grantee inventory disposal*. Except as otherwise provided for in this grant, the Grantee shall not dispose of Grantee inventory until authorized to do so by the Plant Clearance Officer or authorizing official.

(1) Predisposal requirements.

(i) If the Grantee determines that the property has the potential to fulfill requirements under other grants, the Grantee, in consultation with the Property Administrator, shall request that the Granting Officer transfer the property to the grant in question, or provide authorization for use, as appropriate. In lieu of transferring the property, the Granting Officer may authorize the Grantee to credit the costs of Grantee-acquired property (material only) to the losing grant, and debit the gaining grant with the corresponding cost, when such material is needed for use on another grant. Property no longer needed shall be considered Grantee inventory.

(ii) For any remaining Grantee-acquired property, the Grantee may purchase the property at the unit acquisition cost if desired or make reasonable efforts to return unused property to the appropriate supplier at fair market value (less, if applicable, a reasonable restocking fee that is consistent with the supplier's customary practices.)

(2) *Inventory disposal schedules*.

(i) Absent separate grant terms and conditions for property disposition, and provided the property was not reutilized, transferred, or otherwise disposed of, the Grantee, as directed by the Plant Clearance Officer or authorizing official, shall use Standard Form 1428, Inventory Disposal Schedule or electronic equivalent, to identify and report-

(A) Government-furnished property that is no longer required for performance of this grant;

(B) Grantee-acquired property, to which the Government has obtained title under paragraph (e) of this clause, which is no longer required for performance of that grant; and

(C) Termination inventory.

(ii) The Grantee may annotate inventory disposal schedules to identify property the Grantee wishes to purchase from the Government, in the event that the property is offered for sale.

(iii) Separate inventory disposal schedules are required for aircraft in any condition, flight safety critical aircraft parts, and other items as directed by the Plant Clearance Officer.

(iv) The Grantee shall provide the information required by FAR 52.245-1(f)(1)(iii) along with the following:

(A) Any additional information that may facilitate understanding of the property's intended use.

(B) For work-in-progress, the estimated percentage of completion.

(C) For precious metals in raw or bulk form, the type of metal and estimated weight.

(D) For hazardous material or property contaminated with hazardous material, the type of hazardous material.

(E) For metals in mill product form, the form, shape, treatment, hardness, temper, specification (commercial or Government) and dimensions (thickness, width and length).

(v) Property with the same description, condition code, and reporting location may be grouped in a single line item.

(vi) Scrap should be reported by "lot" along with metal content, estimated weight and estimated value.

(3) *Submission requirements*.

(i) The Grantee shall submit inventory disposal schedules to the Plant Clearance Officer no later than-

(A) 30 days following the Grantee's determination that a property item is no longer required for performance of this grant;

(B) 60 days, or such longer period as may be approved by the Plant Clearance Officer, following completion of grant deliveries or performance; or

(C) 120 days, or such longer period as may be approved by the Termination Granting Officer, following grant termination in whole or in part.

(ii) Unless the Plant Clearance Officer determines otherwise, the Grantee need not identify or report production scrap on inventory disposal schedules, and may process and dispose of production scrap in accordance with its own internal scrap procedures. The processing and disposal of other types of Government-owned scrap will be conducted in accordance with the terms and conditions of the grant or Plant Clearance Officer direction, as appropriate.

(4) *Corrections*. The Plant Clearance Officer may-

(i) Reject a schedule for cause (*e.g.*, contains errors, determined to be inaccurate); and

(ii) Require the Grantee to correct an inventory disposal schedule.

(5) *Post-submission adjustments*. The Grantee shall notify the Plant Clearance Officer at least 10 working days in advance of its intent to remove an item from an approved inventory disposal schedule. Upon approval of the Plant Clearance Officer, or upon expiration of the notice period, the Grantee may make the necessary adjustments to the inventory schedule.

(6) *Storage*.

(i) The Grantee shall store the property identified on an inventory disposal schedule pending receipt of disposal instructions. The Government's failure to furnish disposal instructions within 120 days following acceptance of an inventory disposal schedule may entitle the Grantee to an equitable adjustment for costs incurred to store such property on or after the 121st day.

(ii) The Grantee shall obtain the Plant Clearance Officer's approval to remove property from the premises where the property is currently located prior to receipt of final disposition instructions. If approval is granted, any costs incurred by the Grantee to transport or store the property shall not increase the price or fee of any Government grant. The storage area shall be appropriate for assuring the property's physical safety and suitability for use. Approval does not relieve the Grantee of any liability for such property under this grant.

(7) *Disposition instructions*.

(i) The Grantee shall prepare for shipment, deliver f.o.b. origin, or dispose of Grantee inventory as directed by the Plant Clearance Officer. Unless otherwise directed by the Granting Officer or by the Plant Clearance Officer, the Grantee shall remove and destroy any markings identifying the property as U.S. Government-owned property prior to its disposal.

(ii) The Granting Officer may require the Grantee to demilitarize the property prior to shipment or disposal. In such cases, the Grantee may be entitled to an equitable adjustment under paragraph (i) of this clause.

(8) *Disposal proceeds*. As directed by the Granting Officer, the Grantee shall credit the net proceeds from the disposal of Grantee inventory to the grant, or to the Treasury of the United States as miscellaneous receipts.

(9) *Subgrantee inventory disposal schedules*. The Grantee shall require its Subgrantees to submit inventory disposal schedules to the Grantee in accordance with the requirements of paragraph (j)(3) of this clause.

(k) *Abandonment of Government property*.

(1) The Government shall not abandon sensitive property or termination inventory without the Grantee's written consent.

(2) The Government, upon notice to the Grantee, may abandon any non-sensitive property in place, at which time all obligations of the Government regarding such property shall cease.

(3) Absent grant terms and conditions to the contrary, the Government may abandon parts removed and replaced from property as a result of normal maintenance actions or removed from property as a result of the repair, maintenance, overhaul, or modification process.

(4) The Government has no obligation to restore or rehabilitate the Grantee's premises under any circumstances; however, if Government-furnished property is withdrawn or is unsuitable for the intended use, or if other Government property is substituted, then the equitable adjustment under paragraph (i) of this clause may properly include restoration or rehabilitation costs.

(l) *Communication*. All communications under this clause shall be in writing.

(m) *Grants outside the United States.* If this grant is to be performed outside of the United States and its outlying areas, the words "Government" and "Government-furnished" (wherever they appear in this clause) shall be construed as "United States Government" and "United States Government-furnished," respectively.

(End Clause)

Attachment E- 2352.245-1 - Designation of Property Administrator/Listing of Government Property (JUL 2026) - GRANTS

(a) Designation of Property Administrator

(1) TaMika Cleveland is the property administrator for this grant.

(2) TaMika Cleveland is responsible for coordinating property issues with the Government Grant Management Specialist in the Office of Strategic Sourcing, and the Grantee.

(b) Direct questions and/or problems regarding the control of property to TaMika Cleveland at SPSSBA.Rep.Payee.Grants@ssa.gov.

(c) The property administrator cannot obligate Government funds, execute modifications, amendments, or otherwise make changes to the grant.

(d) List of Government property, other than incidental, to be furnished or acquired under this grant:

[TBD at time of grant award]

(End Clause)

Attachment F - Instructions for Secure Disposal of Confidential Information

- **Printed paper records with confidential information must be protected. Understand the policies and procedures concerning protection and loss reporting of confidential information, including personally identifiable information (PII).**
    - Grantees must securely remove and destroy uncollected documents containing confidential information from printing devices at the close of each business day.
    - Grantees must follow the requirements in this award for reporting any lost, compromised, or potentially compromised PII.
- **Printed documents containing PII must be securely destroyed per 36 CFR 1228.58 after the records have been stored electronically in RPMT.**
    - Paper documents containing PII must be destroyed by burning, pulping, shredding, macerating, or other similar means that ensures the destruction of information in the record. Definitively destroy records in a manner that prevents reconstruction and inappropriate use.
    - For in-office shredding, paper should be cross-cut shredded, or strip shredded, to one quarter inch or less prior to disposal by recycling or regular trash.
    - Please note that hand tearing or lining through documents does not meet SSA guidelines for appropriate destruction of PII.
    - Managers should:
        - Remind employees of their responsibilities to shred material containing confidential information.
        - Ensure that their facilities have adequate resources to shred the volume of sensitive material produced by their office, or securely store material pending shredding.
        - Periodically check the office trash and recycle bins to ensure it does not contain confidential information.

(End of Clause)

Attachment G - Guidance and Instructions for Telework

This document establishes the policies and procedures regarding telework policy as it applies to the Protection and Advocacy Systems (P&A) for the SPSSBA grant program administered by the Social Security Administration (SSA). Telework opportunities may be offered provided that the technological components and equipment are available and in place and that sensitive materials, including Personally Identifiable Information (PII), can be safeguarded.

A. Definitions

a. **Telework** - A work arrangement in which personnel perform officially assigned grant duties at their home or other worksite geographically convenient to the Protection and Advocacy organizations commercial business office.
b. **Official Duty Station (ODS)** – The Protection and Advocacy organizations commercial business office where P&A personnel regularly performs their duties.
c. **Alternate Duty Station (ADS) -** A management-approved worksite that is geographically convenient to P&A personnel's ODS. P&A Executive Officers will approve only one ADS per employee. Specifically:
    i. A personnel's residence as reflected in the Telework Program Request or Agreement; or
    ii. Another Protection and Advocacy organization commercial business office that may be closer to the personnel's home.

B. Eligibility

a. Each grantee must develop, maintain, and provide upon request written telework agreements for any staff not working in P&A's commercial business office. The written agreement must include, effective date to begin and end telework and at a minimum the following acknowledgements:
    i. Personnel may only have one ADS that cannot be changed without prior approval of management.
    ii. With the exception of conducting an official onsite representative payee review, an employee may not, perform any grant work in a public setting (e.g., coffee shop, library, shared workspace).
    iii. Personnel may not connect SSA laptop to a public internet/wi-fi source.
    iv. Personnel must report time and attendance in accordance with organization procedures while working at the ADS.
    v. Personnel must maintain ADS worksite in a manner that is conducive to business and is free of hazards. The workspace must include a desk; chair; surge protector; and locking file cabinet, locking desk drawer or other similar secure storage area for official records and information. The personnel are responsible for maintaining adequate workspace, proper lighting, power and other utilities, adequate environmental conditions, adequate security, a working smoke detector, and a readily accessible, working fire extinguisher.
    vi. Personnel is responsible for all operating costs, home maintenance and any other incidental costs (e.g., utilities, high-speed internet access, mortgage payments, rent insurance, and taxes). **Grant funds may not be allocated to pay for these expenses.**
    vii. Personnel understands that all laws, rules, regulations, and agency policies concerning conduct at the ODS remain in full force and effect at the ADS.
    viii. Personnel will not use work time for any purpose other than performing grant-related work. Personnel will have resources necessary to perform job duties and will concentrate on official duties without interruption.

ix. Personnel must comply with **Attachment F – Instructions for Secure Disposal of Confidential Information.** Personnel understands printers may not be used at an ADS. Personnel will comply with terms set forth in P&A IT Equipment Guide.

x. SSA is not liable for damages to personal or real property occurring during the course of performance of duties under this agreement while staff are teleworking.

C. Enrollment

a. The P&A personnel wishing to telework must complete a written request that must be approved and retained by the P&A. The written request should contain the following:
    i. Location of their Alternate Duty Station, if outside of a P&A Office
    ii. Effective date to begin and end telework
b. Any approvals or denials for telework requests will go through the P&A Executive Officer.
c. Written telework requests must be available upon request.
d. Complete telework training video during the Field Office visit during the onboarding credentialing process.

(End Clause)

Attachment H – Privacy, Disclosure, and Security Authorities (AUG2024)

Privacy, Disclosure and Security Authorities Requirements: Table of privacy, disclosure and security laws, regulations, directives, policies, standards, and guidelines.

Authority	Description
Federal Records Act of 1950 and other applicable authorities, 44 U.S.C. §§ 21, 29, 31 and 33	Establishes the framework used by Federal agencies for their Records Management programs.
The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552	This law provides the public with the right to request access to records from any Federal agency and requires that Federal information be made available to the public except under certain specified conditions.
The Privacy Act of 1974, 5 U.S.C. § 552a	This law imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a "system of records." This law also provides an individual a right to access and to amend any information about the individual in a system of records.
Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512	This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.

Authority	Description
Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030	This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers.
Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101	This law establishes policies for managing agency performance of mission, including performance of its practices.
Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520	This law provides for the administration and management of computer resources.
Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401, et seq.	This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government.
Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111	This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.
National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030	This law provides for the protection of computer resources.
Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504	This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic

Authority	Description
	authentication methods to verify the identity of the sender and the integrity of electronic content.
E-Government Act of 2002, 44 U.S.C. § 101	This law enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services.
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3551, as amended by the Federal Information Security Modernization Act of 2014, (Pub. L. 113-283)	FISMA requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

Applicable Programs include but are not limited to:

The Federal Risk and Authorization Management Program (FedRAMP)	FedRAMP is a Federally centralized risk management program that enforces a standardized approach for assessing and monitoring the FISMA compliance of cloud products and services. The FedRAMP program requires cloud providers to receive an independent security assessment, conducted by a third- party assessment organization (3PAO), to sell government cloud services to a federal agency.

CUI Registry	Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, Federal regulations, and Government-wide policies.

Applicable Executive Orders include but are not limited to:

Executive Order 10450, Security Requirements for Government Employment, April 1953, as repealed in part by Executive Order 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters, January 2023	These orders establish that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	This order establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, September 1998	This order establishes policy that each executive agency shall work diligently to prevent and combat software piracy to give effect to copyrights associated with computer software.

Presidential Decision Directive 63/NSC: Critical Infrastructure Protection, May 1998	This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber-attacks on critical infrastructures, including our cyber systems.
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.
Executive Order 14028, Improving the Nation's Cybersecurity, May 2021	Aims to improve the nation's cybersecurity. It requires the Federal Government to enhance efforts in identifying, deterring, protecting against, detecting, and responding to malicious cyber campaigns. The order mandates the adoption of secure cloud services, zero- trust architecture, and deployment of multifactor authentication and encryption within specific timeframes. Additionally, it establishes a Federal Cybersecurity Framework to guide agencies in protecting their systems and data.

Executive branch policies established through directives published by OMB based on the applicable laws passed by Congress include:

OMB Circular	Description
A-11, Section 53, Information Technology and E-Government	This directive specifies the identification of security and privacy safeguards for managing sensitive information.

A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, as revised July 2016	This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-123, Appendix D, M-13-23, Compliance with the Federal Financial Management Improvement Act of 1996	This directive prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix I, Managing Information as a Strategic Resource	This directive prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII).

Other requirements:

OMB Memorandum M-05-24, Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Recipients.

OMB Memorandum M-08-05, Implementation of Trusted Internet Connections, which establishes the requirement for SSA to comply with the Trusted Internet Connection (TIC) initiative and the architectural requirements defined by the Department of Homeland Security (DHS) in the TIC Reference Architecture (current version 2.0 dated 2011).

OMB Memorandum M-08-16, Guidance for Trusted Internet Connection (TIC) Statement of Capability Form.

OMB Memorandum M-08-27, Guidance for Trusted Internet Connection Compliance.

OMB Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Recipients.

OMB M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.

OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.

OMB M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

OMB Memorandum M-21-30, Protecting Critical Software Through Enhanced Security Measures

OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

OMB Memorandum M-23-22, Delivering a Digital-First Public Experience

OMB proposed guidance, Improving Cybersecurity Protections in Federal Acquisitions.

National Security Presidential Directive and Homeland Security Presidential Directive (NSPD-54/HSPD-23), Comprehensive National Cyber Security Initiative.

Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Recipients.

Department of Homeland Security (DHS) Trusted Internet Connection (TIC), Version 2.0, Reference Architecture requirements.

Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance and associated NIST standards regarding implementation and use of HSPD-12 Personal Identity Verification (PIV) two-factor SmartCard Public Key Infrastructure (PKI) based credentials for logical authentication.

NIST Federal Information Processing Standard (FIPS) Publications.

NIST 800-series Special Publications (SP).

NIST Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists).

All management, operational and technical security control and continuous monitoring requirements as specified by FedRAMP.

Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance.

SSA TIC security architecture.

(End Clause)

Attachment I – Notice of Specific Terms and Conditions for Risk Tiered Awards (2026)

NOTICE TO GRANTEES: IMPOSITION OF SPECIFIC CONDITIONS BASED ON PERFORMANCE RISK TIER

Pursuant to 2 C.F.R. 200.208, the agency may impose specific conditions on this award based on an analysis of factors such as your organization's compliance history, demonstrated ability to meet performance goals, financial capability, and information obtained from government-wide data sources. This notice serves as a formal warning that if your Notice of Award (NOA) specifies a risk-tier identified in the Remarks section the corresponding specific conditions outlined below will be applied to your award. If your organization is identified as high risk during the current budget period, an amended NOA will be issued, identifying the risk level in the Remarks section of the award document.

The performance measures described in this notice will apply to any assessment of performance for a Protection and Advocacy (P&A) organization. These measures will be used to determine risk tier assignment and the imposition of specific conditions.

Risk Factors
The evaluation of your organization's past performance has identified the following risk factors: see attached table for criteria and risk tier assignment.

Imposition and Removal of Specific Conditions
The specific conditions outlined in this notice are being imposed to address the identified risks and to ensure the effective management and oversight of federal funds. Once the conditions that prompted these requirements have been satisfied, the agency will promptly remove them.

TERMS AND CONDITIONS: SPECIFIC CONDITIONS BY RISK TIER

GENERAL PROVISIONS

The awarding agency reserves the right to modify, add, or remove specific conditions as necessary to ensure compliance with federal requirements to mitigate risk, in accordance with 2 C.F.R. 200.208.

If your NOA indicates a risk tier, you are required to comply with the corresponding specific conditions as described below.

The recipient will be notified in writing of any changes to their risk tier or specific conditions, including the rationale for such changes and actions required to return to standard conditions. SSA will maintain documentation supporting the basis for the imposition of specific conditions.

Risk Tier Criteria and Corresponding Conditions

Criteria	Risk Tier			
	0	**1**	**2**	**3**
Overall Completion of Target (Previous Year) The number and types of reviews completed during the immediately preceding grant year in relation to the SSA approved workplan prescribed in the program narrative of the annual grant application.	>80%	71%-80%	60%-70%	< 60%
Periodic Reviews Completed (Previous Year) The number of periodic reviews released during the previous grant year compared to the number of those review that were completed within the same period.	>80%	71%-80%	60%-70%	< 60%
Periodic Reviews Completed (Older than One Year) The percentage of periodic reviews assigned more than one year ago that have been completed.	>99%	96%-99%	90%-95%	< 90%
Review Quality Compliance The extent to which completed reviews conform to the processes, procedures, and timeframes established in the Business Process Document, as measured by the percentage of cases submitted to the NAG Final Review stage in RPMT that do not require return to the P&A for correction.	>80%	71%-80%	60%-70%	<60%
Comparative Performance Performance outcomes as measured by evaluating each grantee's results and program expectations across key performance measures alongside those of similarly sized organizations or national averages. To ensure that performance is assed accurately and equitably, the risk tier for each metric will be determined using the most appropriate statistical method based on the nature and distribution of the data. Examples of such methods include calculating percentage differences, standard deviations from the mean, or percentile rankings within the dataset.	Within typical or expected range	Moderately below	Significantly below	Substantially below

Specific Conditions by Risk Tier

Tier 1: Enhanced Monitoring

- The recipient must:
    - Participate in additional project monitoring, including mandatory attendance (virtual) at recurring performance touchpoints with SSA staff as scheduled by the awarding agency.

Tier 2: Enhanced Monitoring & Reporting

- In addition to all Tier 1 requirements, the recipient must:
    - Participate in mandatory technical assistance sessions provided by the National Association Grantee (NAG).
    - Submit monthly reports on the status of past due cases identified by SSA, in a format specified by the awarding agency.
        - Submit monthly reports detailing progress towards deliverables as outlined in the work plan of the grant agreement.

Tier 3: Enhanced Monitoring, Reporting, and Additional Restrictions

- In addition to all Tier 1 and Tier 2 requirements, the recipient is subject to the following conditions:
    - The recipient's authority to work on non-priority cases is withheld until evidence of acceptable performance is provided, as determined by SSA.
    - The recipient will provide a Corrective Action Plan to SSA which will include a description of priority cases within 30 days of this award.
    - The recipient must prioritize cases as directed by SSA and may not engage in other non-priority activities without SSA's prior approval.
    - The recipient must obtain prior written approval from the SSA Program Officer before performing work on non-priority cases, non-case work activities, or non-essential administrative functions (including but not limited to conferences, training, and similar activities).
    - Payments to the recipient will be on a *reimbursement basis only*. Advance payments are not permitted.
    - All reimbursed expenses must be directly related to work on priority cases as directed by SSA unless the activity has received prior written approval from the SSA Program Officer.

NONCOMPLIANCE & TERMINATIONS

If the recipient fails to improve performance and comply with the corrective action plan or the specific conditions imposed, the awarding agency may seek remedies for non-compliance as outlined in Item 24 – Noncompliance and Terminations of the General Terms and Conditions of this award, and as provided in 2 C.F.R. 200.339.

RECONSIDERATION PROCESS FOR SPECIFIC CONDITIONS

Opportunity to Request Reconsideration
The grantee may submit a written request for reconsideration to the SSA Grants Management Officer within fifteen (15) calendar days. The request must include supporting information and documentation explaining why the imposition of the specific conditions is not necessary.

Agency Review and Final Determination
The awarding agency will review the recipient's request and supporting materials. The agency will provide a written response within thirty (30) calendar days of receipt of the request, stating the basis for its decision to uphold, modify, or remove the specific conditions. The recipient must comply with the final determination regarding the specific conditions.

(End Clause)