

NOTIFICATION OF PERSONNEL ACTION

|   |              |  |                  |  |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
|---|--------------|--|------------------|--|---|-----------------------------------|--------------------------------|---|---------------------------------|---|---------------------|-----------------------------------|--|--------------------------|--|
| 1. Name (Last, First, Middle)<br>Employee 1   |              |  |                  |  | 2. Social Security Number<br>[REDACTED]   |                                   | 3. Date of Birth<br>[REDACTED] |   | 4. Effective Date<br>02/09/2025 |   |                     |                                   |  |                          |  |
| FIRST ACTION  |              |  |                  |  | SECOND ACTION   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 5-A. Code<br>171  |              | 5-B. Nature of Action<br>EXC APPT NTE 02-08-26 |                  |  | 6-A. Code   |                                   | 6-B. Nature of Action          |   |                                 |   |                     |                                   |  |                          |  |
| 5-C. Code<br>ZLM  |              | 5-D. Legal Authority<br>5 U.S.C. 3109          |                  |  | 6-C. Code   |                                   | 6-D. Legal Authority           |   |                                 |   |                     |                                   |  |                          |  |
| 5-E. Code   |              | 5-F. Legal Authority                           |                  |  | 6-E. Code   |                                   | 6-F. Legal Authority           |   |                                 |   |                     |                                   |  |                          |  |
| 7. FROM: Position Title and Number  |              |  |                  |  | 15. TO: Position Title and Number<br>EXPERT<br>EXPERT<br>S4C KNX0350  |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 8. Pay Plan   | 9. Occ. Code | 10. Grade or Level                             | 11. Step or Rate | 12. Total Salary   | 13. Pay Basis   | 16. Pay Plan<br>ED                | 17. Occ. Code<br>0301          | 18. Grade or Level<br>00                    | 19. Step or Rate<br>00          | 20. Total Salary/Award<br>\$90025.00              | 21. Pay Basis<br>PA |                                   |  |                          |  |
| 12A. Basic Pay  |              | 12B. Locality Adj.                             |                  | 12C. Adj. Basic Pay  |   | 12D. Other Pay                    |                                | 20A. Basic Pay<br>\$90025.00                |                                 | 20B. Locality Adj.<br>\$0.00                      |                     | 20C. Adj. Basic Pay<br>\$90025.00 |  | 20D. Other Pay<br>\$0.00 |  |
| 14. Name and Location of Position's Organization  |              |  |                  |  | 22. Name and Location of Position's Organization<br>SZ00 SOCIAL SECURITY ADMINISTRATION<br>CHIEF INFORMATION OFFICER<br>OFFICE OF CHIEF INFORMATION OFFICER |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| EMPLOYEE DATA   |              |  |                  |  |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 23. Veterans Preference<br>1 1 - None 3 - 10-Point/Disability 5 - 10-Point/Other<br>2 - 5-Point 4 - 10-Point/Compensable 6 - 10-Point/Compensable/30%   |              |  |                  |  | 24. Tenure<br>0 0 - None 2 - Conditional<br>1 - Permanent 3 - Indefinite  |                                   |                                | 25. Agency Use                              |                                 | 26. Veterans Preference for RIF<br>YES X NO       |                     |                                   |  |                          |  |
| 27. FEGLI<br>A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERAGE   |              |  |                  |  | 28. Annuitant Indicator<br>9 NOT APPLICABLE   |                                   |                                |   |                                 | 29. Pay Rate Determinant<br>0                     |                     |                                   |  |                          |  |
| 30. Retirement Plan<br>2 FICA   |              |  |                  | 31. Service Comp. Date (Leave)<br>02/09/2025   |   | 32. Work Schedule<br>F FULL-TIME  |                                |   |                                 | 33. Part-Time Hours Per<br>Biweekly<br>Pay Period |                     |                                   |  |                          |  |
| POSITION DATA   |              |  |                  |  |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 34. Position Occupied<br>2 1 - Competitive Service 3 - SES General<br>2 - Excepted Service 4 - SES Career Reserved  |              |  |                  | 35. FLSA Category<br>N E - Exempt<br>N - Nonexempt   |   | 36. Appropriation Code<br>4003431 |                                |   |                                 | 37. Bargaining Unit Status<br>8888                |                     |                                   |  |                          |  |
| 38. Duty Station Code<br>24-1698-005  |              |  |                  | 39. Duty Station (City - County - State or Overseas Location)<br>WOODLAWN,BALTIMORE,MARYLAND |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 40. Agency Data<br>FUNC CLS 00  |              | 41. VET STAT X                                 |                  | 42. EDUC LVL   |   | 43. SUPV STAT 8                   |                                | 44. POSITION SENSITIVITY CRITICAL-SENSITIVE |                                 |   |                     |                                   |  |                          |  |
| 45. Remarks<br>APPOINTMENT AFFIDAVIT EXECUTED 02/10/25.<br>PREVIOUS RETIREMENT COVERAGE: NEVER COVERED<br>REASON FOR TEMPORARY APPOINTMENT TO PERFORM ANALYSIS OF SSA PAYMENT DATA TO<br>REDUCE CONCERNS RAISED BY THE ADMINISTRATION.<br>CREDITABLE MILITARY SERVICE: NONE<br>YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES. |              |  |                  |  |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 46. Employing Department or Agency<br>SZ - SOCIAL SECURITY ADMIN  |              |  |                  |  | 50. Signature/Authentication and Title of Approving Official<br>250644169 / ELECTRONICALLY SIGNED BY:<br>[REDACTED]<br>DIRECTOR, OESS                       |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |
| 47. Agency Code<br>SZ00   |              | 48. Personnel Office ID<br>1166                |                  | 49. Approval Date<br>02/09/2025  |   |                                   |                                |   |                                 |   |                     |                                   |  |                          |  |

2/13/25

1

EXPERT OR CONSULTANT  
APPOINTMENT REQUEST & CERTIFICATION

|   |  |
|---|--|
| 1. NAME OF PERSON (Last, first, middle initial)<br>2. <b>Employee 1</b> | 2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED 365                                       |
| 3. MAILING ADDRESS  | 4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 |

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL THE SERVICES TO BE PERFORMED.

Access to all SSA systems and the associated source code to assist with modernization efforts agreed to by the CIO

The duties relate to improper payments and the Death Master File. Below is a beginning description, but this is a work in progress:

1. Evaluate the existence of matches between the agency's pay list and the Death Master File and analyze the causes. If matches are found offer recommendations for improvements.
2. Evaluate the existence of matches between the agency's pay list and the "Do Not Pay" file and analyze causes. If matches are found offer recommendations for improvements.
3. Assess the current process used by SSA to obtain information for the Death Master File and offer recommendations for improvement of the process by which information is obtained.
4. Prepare recommendations related to the duties above and without using the active production system, provide examples of code improvements.

**Employee 1** will be performing analysis of SSA payment data to reduce concerns raised by the administration. This will include analyzing our current payments to beneficiaries against other SSA records to identify potential improper payments. Data needed to perform the analysis will be SSA payment files sent to Treasury and potentially the Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR). Security controls will be implemented to prevent **Employee 1** from accessing or viewing sensitive data within any of these records.

B. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE TRANSACTION OF BUSINESS ON BEHALF OF THE GOVERNMENT WITH ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

C. SPECIFY WHAT DUTIES WILL BE ASSIGNED THAT WILL INVOLVE THE PERSON IN THE RENDERING OF ADVICE TO THE GOVERNMENT WHICH WILL HAVE DIRECT AND PREDICTABLE EFFECT ON THE INTERESTS OF ANY PROFIT OR NON-PROFIT ORGANIZATION.

None

6. SPECIAL QUALIFICATIONS OF THE PERSON RECOMMENDED FOR APPOINTMENT (List those which relate specifically to the services to be performed.)

Hands-on software engineer that is an expert in modern computer programming languages, cloud and other infrastructure, AI, etc.

5 years of experience using numerous computer code languages, leadership of teams in technical, software design, and infrastructure areas.

2/13/25

2

## CERTIFICATION

In approving the appointment of this consultant/expert, I have considered the requirements of law, relevant decisions of the Comptroller General, and Office of Personnel Management Department policies and instructions. More specifically, I have satisfied myself that:

1. The services of the individual are essential for effective program management
2. The duties to be performed are those of (check one)
  - ☐ a consultant (that is, they are purely advisory in nature and will not include the performance or supervision of operating functions)
  - ☒ an expert (that is, they require a high level of expertise not available in the regular work force)
3. The proposed appointee is qualified to (check one)
  - ☐ provide advisory services as a consultant under 5 CFR 304
  - ☒ serve as an expert under 5 CFR 304
4. The appointment is appropriately designated as (check one)
  - ☐ Intermittent not to exceed 1 year (the individual will work occasionally and irregularly) not to exceed the equivalent of 6 months.
  - ☐ Part-time not to exceed 1 year.
  - Provide tour: \_\_\_\_\_
  - ☒ Full-time not to exceed 1 year
5. The appropriate appointment authority is being used
6. The pay level is GS grade/step 13/1 equivalent. This is appropriate for the duties to be performed and the qualifications of the appointee (Minimum GS 13/1 base salary. Maximum GS-15/10 base salary.)
  - ☐ Appointee will waive compensation (attach written agreement)
7. The record of appointment has been clearly documented to show the services to be performed and the special qualifications of the appointee which relate specifically to those services.
8. A statement of employment and financial interests has been obtained and it has been determined that no conflict of interest exists (OGE Form 450 was reviewed. Components retain this form).

Date

2/13/25

\_\_\_\_\_  
 Signature of Component Program Manager Authorized to Obtain the  
 Consultant's/Expert's Services (This certification relates particularly to  
 items 1, 2, 3, 6, 7 and 8)

Date

2/13/25

\_\_\_\_\_  
 Signature of DCHRCPPS Appointing Official (This certification relates  
 particularly to items 2 through 8)



# APPOINTMENT AFFIDAVITS

Expert  
(Position to which Appointed)

02/10/2025  
(Date Appointed)

Social Security Administration  
(Department or Agency)

Office of the Chief Information  
(Bureau or Division)

Woodlawn, Maryland  
(Place of Employment)

I, **Employee 1**, do solemnly swear (or affirm) that--

## A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

## B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

## C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

**Employee 1**

(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 10th day of February, 2025

at Woodlawn  
(City)

Maryland  
(State)

(SEAL)

(Signature of Officer)

Commission expires \_\_\_\_\_  
(If by a Notary Public, the date of his/her Commission should be shown)

Deputy Commissioner for Human Resour  
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

## Information Security and Privacy Awareness / Rules of Behavior

### Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

### Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

### Safeguarding Sensitive Information

**Sensitive Information** is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external 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.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

---

### Public Disclosure

---

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive 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; and
- 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.

---

### Alternative Worksite (Non-SSA Controlled Locations)

---

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

---

### Social Engineering

---

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.  
Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

---

### Awareness and Training

---

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.



**Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion**

**SSA Employees** - Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: Employee 1

Last Name: Employee 1

Day Phone:

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Information Security Awareness / Rules of Behavior completed:

Signature: Employee 1

Date:

02/10/2025

*If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.*