Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle)	2. Social Security Number	3. Date of Birth	4. Effective Date
Employee 4	[redacted]	[redacted]	02/23/2025

FIRST ACTION

5–A. Code	5–B. Nature of Action	6–A. Code	6–B. Nature of Action
002	CORRECTION	171	EXC APPT NTE 02-22-26
5–C. Code	5–D. Legal Authority	6–C. Code	6–D. Legal Authority
		H2L	REG 304.103
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
	EXPERT EXPERT S4C KNX0370

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis	16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
						ED	0301	00	00	$0.00	WC

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay	20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
				$0.00	$0.00	$0.00	$0.00

14. Name and Location of Position's Organization	22. Name and Location of Position's Organization
	SZ00 SOCIAL SECURITY ADMINISTRATION CHIEF INFORMATION OFFICER OFFICE OF CHIEF INFORMATION OFFICER

EMPLOYEE DATA

23. Veterans Preference	24. Tenure	25. Agency Use	26. Veterans Preference for RIF
1 (1 – None, 2 – 5–Point, 3 – 10–Point/Disability, 4 – 10–Point/Compensable, 5 – 10–Point/Other, 6 – 10–Point/Compensable/30%)	0 (0 – None, 1 – Permanent, 2 – Conditional, 3 – Indefinite)		YES [ ] X NO

27. FEGLI	28. Annuitant Indicator	29. Pay Rate Determinant
A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERA	9 NOT APPLICABLE	0

30. Retirement Plan	31. Service Comp. Date (Leave)	32. Work Schedule	33. Part–Time Hours Per Biweekly Pay Period
2 FICA	02/23/2025	I INTERMITTENT	

POSITION DATA

34. Position Occupied	35. FLSA Category	36. Appropriation Code	37. Bargaining Unit Status
2 (1 – Competitive Service, 2 – Excepted Service, 3 – SES General, 4 – SES Career Reserved)	E (E – Exempt, N – Nonexempt)	4003431	8888

38. Duty Station Code	39. Duty Station (City – County – State or Overseas Location)
24-1698-005	WOODLAWN,BALTIMORE,MARYLAND

40. Agency Data	41.	42.	43.	44.
FUNC CLS 00	VET STAT X	EDUC LVL	SUPV STAT 8	POSITION SENSITIVITY CRITICAL-SENSITIVE

45. Remarks
CORRECTS ITEM 1 TO READ: Employee 4

46. Employing Department or Agency	50. Signature/Authentication and Title of Approving Official
SZ - SOCIAL SECURITY ADMIN	250928535 / ELECTRONICALLY SIGNED BY: [redacted] DIRECTOR, OESS

47. Agency Code	48. Personnel Office ID	49. Approval Date
SZ00	1166	03/13/2025

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Previous Edition Not Usable After 6/30/93
NSN 7540–01–333–6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296–33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle)	2. Social Security Number	3. Date of Birth	4. Effective Date
Employee 4	[redacted]	[redacted]	02/23/2025

FIRST ACTION

5–A. Code	5–B. Nature of Action	6–A. Code	6–B. Nature of Action
171	EXC APPT NTE 02-22-26		
5–C. Code	**5–D. Legal Authority**	**6–C. Code**	**6–D. Legal Authority**
H2L	REG 304.103		
5–E. Code	**5–F. Legal Authority**	**6–E. Code**	**6–F. Legal Authority**

SECOND ACTION

7. FROM: Position Title and Number	15. TO: Position Title and Number
	EXPERT EXPERT S4C KNX0370

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ED	0301	00	00	$0.00	WC

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$0.00	$0.00	$0.00	$0.00

14. Name and Location of Position's Organization	22. Name and Location of Position's Organization
	SZ00 SOCIAL SECURITY ADMINISTRATION CHIEF INFORMATION OFFICER OFFICE OF CHIEF INFORMATION OFFICER

EMPLOYEE DATA

23. Veterans Preference	24. Tenure	25. Agency Use	26. Veterans Preference for RIF
1 (1 – None; 2 – 5–Point; 3 – 10–Point/Disability; 4 – 10–Point/Compensable; 5 – 10–Point/Other; 6 – 10–Point/Compensable/30%)	0 (0 – None; 1 – Permanent; 2 – Conditional; 3 – Indefinite)		YES: ; NO: X

27. FEGLI	28. Annuitant Indicator	29. Pay Rate Determinant
A0 EMPLOYEE IN A POSITION EXCLUDED FROM FEGLI COVERAG	9 NOT APPLICABLE	0

30. Retirement Plan	31. Service Comp. Date (Leave)	32. Work Schedule	33. Part–Time Hours Per Biweekly Pay Period
2 FICA	02/23/2025	I INTERMITTENT	

POSITION DATA

34. Position Occupied	35. FLSA Category	36. Appropriation Code	37. Bargaining Unit Status
2 (1 – Competitive Service; 2 – Excepted Service; 3 – SES General; 4 – SES Career Reserved)	E (E – Exempt; N – Nonexempt)	4003431	8888

38. Duty Station Code	39. Duty Station (City – County – State or Overseas Location)
24-1698-005	WOODLAWN,BALTIMORE,MARYLAND

40. Agency Data	41.	42.	43.	44.
FUNC CLS 00	VET STAT X	EDUC LVL	SUPV STAT 8	POSITION SENSITIVITY CRITICAL-SENSITIVE

45. Remarks

APPOINTMENT AFFIDAVIT EXECUTED 02-24-25.
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
REASON FOR TEMPORARY APPOINTMENT REVIEW PRIOR AUDITS AND STUDIES CONCERNING
IMPROVEMENTS TO SSA'S NUMIDENT DEATH RECORDS AND ASSESS THE CURRENT
PROCESS USED BY SSA TO OBTAIN DEATH INFORMATION FOR SSA'S PROGRAMS
AND OFFER RECOMMENDATIONS FOR IMPROVEMENT.
CONDUCT ANALYSIS OF SSA PAYMENT DATA TO REDUCE CONCERNS IMPROPER
PAYMENTS
YOU ARE SUBJECT TO REGULATIONS GOVERNING CONDUCT AND RESPONSIBILITIES OF SPECIAL GOVERNMENT EMPLOYEES.

46. Employing Department or Agency	50. Signature/Authentication and Title of Approving Official
SZ - SOCIAL SECURITY ADMIN	250727437 / ELECTRONICALLY SIGNED BY:

47. Agency Code	48. Personnel Office ID	49. Approval Date	
SZ00	1166	02/23/2025	[redacted] DIRECTOR, OESS

5–Part 50–316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540–01–333–6238

EXPERT OR CONSULTANT
APPOINTMENT REQUEST & CERTIFICATION
(Submit with Resume)

1. NAME OF PERSON *(Last, first, middle initial)* Employee 4	2. TOTAL PERIOD FOR WHICH APPOINTMENT IS REQUESTED *(entire year (365) days or a shorter period). List dates from beginning to end month/day/year.* 365 days
3. MAILING ADDRESS [redacted]	4. APPROXIMATE NUMBER OF DAYS PERSON IS EXPECTED TO PERFORM SERVICES DURING THIS PERIOD. 365 days

5. SERVICES TO BE PERFORMED

A. EXPLAIN IN FULL DETAIL THE NON-CONTINUOUS/TEMPORARY NATURE OF THE WORK TO BE PERFORMED AND THE NECESSITY FOR THE POSITION TO ACTUALLY REQUIRE AN EXPERT'S OR CONSULTANT'S SERVICES AS OPPOSED TO A REGULAR GOVERNMENT EMPLOYEE, OR IN THE CASE OF A REAPPOINTMENT (WITH SAME DUTIES), THE CONTINUING NEED FOR THE SERVICES OF AN EXPERT OR CONSULTANT (AND HOURS/DAYS WORKED IN PRECEDING YEAR).

SSA is facing significant issues that require immediate attention. Two of the most substantial areas in need of timely attention include: (1) Numident records with death data and (2) Payment data, focused on reducing improper payments.

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.

1. Examine the recent Ernst & Young audit of SSA.

2. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

3. Evaluate the death information available on SSA's Numident record with death data available in "Do Not Pay" file and analyze any data differences. If necessary, offer recommendations for improvements;

4. Review prior audits and studies concerning improvements to SSA's Numident death records and assess the current process used by SSA to obtain death information for SSA's programs and offer recommendations for improvement of the process by which information is obtained;

5. Prepare recommendations related to the duties above and, without using the active production system, provide examples of code improvements;

6. Conduct analysis of SSA payment data to reduce concerns improper payments. This will include analyzing data of SSA current payments to beneficiaries against other SSA records to identify potential improper payments; and

7. 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 detailee from accessing or viewing sensitive data within any of these records.

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.*

Employee 4 is the Founder, Chief Executive Officer, and Chief Investment Officer of [redacted] founded [redacted] in [redacted] He has over 25 years of experience in private equity investing. Employee 4 was a Director of [redacted] During his tenure, he served as [redacted] He is a Director of [redacted]. He is a member of [redacted].

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 service of the expert or consultant does not duplicate any previously performed work or service, and that the service is not currently available within SSA

3. 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)

   X__an expert (that is, they require a high level of expertise not available in the regular work force)

4. The proposed appointee has a high degree of attainment in the field and is qualified to (check one):

   ___provide advisory services as a consultant under 5 CFR 304

   X__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 expert and consultant appointing authority is the most appropriate authority to use

6. The pay level is GS grade/step _15/10_____ 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.)

   _X__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 will be obtained to determine if any conflict of interest exists (OGE Form 450 will be obtained after onboarding. Components retain OGC comments).

Michael Russo Digitally signed by Michael Russo Date: 2025.02.24 17:44:54 -05'00'

Date — 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)

2/27/25 [redacted]

Date — Signature of DCHR Appointing Official (This certification relates particularly to items 2 through 8)

ADDENDUM TO THE EXPERT/CONSULTANT APPOINTMENT REQUEST AND CERTIFICATION

1. During Appointee's term of service to SSA, Appointee voluntarily waives compensation, as described in the Appointment Request and Certification, from SSA.

2. While on duty time at SSA, Appointee shall only perform duties for SSA.

3. While on duty time for SSA or at SSA Headquarters (HQ) Woodlawn, Maryland, Appointee shall not perform any work for or on behalf of any other entity, government or private.

4. Appointee shall perform SSA work only at SSA Headquarters (HQ) in Woodlawn, Maryland.

5. SSA shall provide any necessary equipment or systems access to ensure access to SSA systems consistent with the Appointee's specific duties as described in the Appointment Request and Certification.

6. Appointee shall not perform any non-SSA work using SSA equipment or resources.

7. Appointee shall not perform SSA work non-SSA equipment or resources.

8. Appointee shall not share any Personally Identifiable Information accessed or obtained through the use of SSA systems or work performed for SSA, with any external entity, organization, or agency federal or state.

9. Appointee shall not share or disclose SSA information that is non- PII, non-public information with any non-federal entity. Any disclosure of non- PII, non-public information to another federal entity, organization, or agency shall be made only with expressed permission of the Office of the Commissioner.

10. Appointee shall abide by all SSA regulations and policies regarding access to and protection of any agency records, information, and work products.

11. Appointee shall abide all SSA regulations and policies regarding ethics and employee conduct.

12. In the event of any lapse in appropriations, the Appointee will follow the instructions issued by SSA related to his SSA service.

APPOINTMENT AFFIDAVITS

Expert
(Position to which Appointed)

02/23/2025
(Date Appointed)

Social Security Administration | Office of the Chief Informatio | Woodlawn, Maryland
(Department or Agency) | *(Bureau or Division)* | *(Place of Employment)*

I, Employee 4, 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 4

Subscribed and sworn (or affirmed) before me this 24 day of February, 2025

at Woodlawn (City) Maryland (State)

[redacted]
(Signature of Officer)

(SEAL)

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

Director, Office of Executive and Special
(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.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

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.

Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

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 4

Last Name: [redacted]

Day Phone: [redacted]

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:

Signatu[redacted] Employee 4 | Date: 2/24/202[illegible]

If yo[redacted]r illegible, or if your signature is omitted, this form will not be p[redacted]