Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Personally Identifiable Information Loss Reporting

042401 September 2025

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 18, 2025 **Refer to:** 042401

To: Frank Bisignano
Commissioner

From: Michelle L. Anderson
Acting Inspector General

Subject: Personally Identifiable Information Loss Reporting

The attached final report presents the results of the Office of Audit's review. The objective was to determine whether Social Security Administration employees properly responded to losses of personally identifiable information.

Please provide within 60 days a corrective action plan that addresses each recommendation. If you wish to discuss the final report, please contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

Personally Identifiable Information Loss Reporting 042401

September 2025 **Office of Audit Report Summary**

Objective

To determine whether Social Security Administration (SSA) employees properly responded to losses of personally identifiable information (PII).

Background

PII is any information SSA maintains about an individual that can be used to distinguish or trace their identity. Federal laws and regulations require that SSA protect PII and to report when losses occur.

SSA's *Breach Response Plan* establishes a framework for responding to a loss of PII. SSA employees must report a loss of PII to their manager or designated official within 1 hour of its loss. The manager's responsibilities include determining whether the issue needs to be reported; using SSA's loss reporting tool to report suspected or confirmed loss; and taking other actions, such as reporting specific types of losses to the Office of the Inspector General (OIG). Designated Breach Response Coordinators work with managers and SSA's Office of Privacy and Disclosure to determine the risk of harm to individuals or SSA.

We identified 2 sampling frames from a total of 27,180 PII Loss Reports in Calendar Years 2019 to 2023. Sampling Frame 1 comprised 658 loss reports not included in SSA's legacy loss reporting tool. Sampling Frame 2 comprised 26,522 reports included in SSA's legacy loss reporting tool.

Results

SSA employees reported 23,954 (88 percent) of the PII losses from Calendar Years 2019 to 2023 in the legacy loss reporting tool with an assessed risk level as required. However, employees did not properly record 658 PII losses (2 percent) in the legacy loss reporting tool or assign a risk level to another 2,568 open loss reports (10 percent). On average, these open loss reports remained pending for 657 days. Additionally, of the 120 loss reports we reviewed, SSA referred 4 (3 percent) to the OIG as required and did not refer 32 (27 percent) as required. (The remaining loss reports did not need to be referred to OIG.)

Conclusion

The Agency needs to update its guidance and evaluate the effectiveness of its updated processes and controls to ensure employees respond to PII losses properly. By appropriately reporting, assessing, and referring suspected or confirmed PII losses, employees can help mitigate the potential harm to individuals and the Agency.

Recommendations

We made three recommendations including

1. distribute the 658 PII losses in Sampling Frame 1 to the appropriate component(s) for review to determine whether any losses are moderate, high, or major, and, if so, identify and take the proper actions to mitigate those losses;

2. to prevent future employee errors related to reporting, assessing, and closing PII losses, evaluate the effectiveness of the processes and controls implemented by the Office of Privacy and Disclosure and implement changes as needed; and

3. update the *Breach Response Plan* to clearly explain all actions relevant to OIG referrals, such as when managers should use forms related to lost or stolen equipment.

SSA agreed to implement our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

C.F.R.	Code of Federal Regulations
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPD	Office of Privacy and Disclosure
PII	Personally Identifiable Information
SSA	Social Security Administration
U.S.C.	United States Code

OBJECTIVE

To determine whether Social Security Administration (SSA) employees properly responded to losses of personally identifiable information (PII).

BACKGROUND

PII is any information SSA maintains about an individual that can be used to distinguish or trace their identify, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records and other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Federal laws and regulations require that SSA protect PII and report when this information is stored, how it is protected, and when breaches occur.[1]

Responding to Losses

PII losses occur when any information that contains PII leaves SSA's custody or is disclosed to an unauthorized individual/entity. SSA's *Breach Response Plan* establishes a framework for responding to a loss of PII.[2] SSA employees must report a PII loss to their manager or designated official within 1 hour of its loss. The manager's responsibilities include determining whether the issue needs to be reported; reporting the suspected or confirmed loss using the loss reporting tool; and taking other actions, such as filing a police report for stolen items and reporting specific types of losses to the Office of the Inspector General (OIG).[3]
Employees should report the loss in rare instances when they cannot reach a manager or designated official.[4]

[1] 44 U.S.C. §§ 3501, 3506, 20 C.F.R.§ 401.30. A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purpose (SSA, *Breach Response Plan*, sec. 5, p. 5 (June 2017)). For the remainder of the report, we use the term "loss."

[2] SSA updated its Breach Response Plan during our audit in 2024. We used the 2017 Breach Response Plan for our sample review.

[3] SSA replaced the PII Loss Reporting Tool with ServiceNow on March 28, 2025. For consistency, we refer to this system as the loss reporting tool throughout this document. We refer to the original tool as the "legacy loss reporting tool" in this document.

[4] SSA, *Breach Response Plan*, sec. 6, pp. 6-7 (June 2017).

Reporting Losses and Assessing Risk

SSA employees must record all reportable PII losses in SSA's loss reporting tool.[5] If the tool is not available, employees must report the loss to SSA's service center via telephone and update the loss reporting tool when it becomes available.[6] All SSA employees must receive privacy and information security awareness training before they access SSA's information systems and annually to maintain access.[7]

Most losses the Agency experiences are routine, unintended disclosures of PII and can quickly be assessed as low risk and closed out. However, depending on the potential impact to individuals or the Agency, a thorough risk of harm assessment may be needed.
Each component must designate breach response coordinators, who work with the appropriate managers and SSA's Office of Privacy and Disclosure (OPD) to determine the risk of harm to individuals or SSA.[8]

The Agency's *Breach Response Plan* explains the risk factors and how to assign risk levels. When assessing the risk level of a loss, employees must consider possible harms, such as identity theft, the potential for blackmail, physical harm, and emotional distress, that may result from the potential misuse of PII by unauthorized individuals. Based on the risk of harm assessment and consultation with Agency leadership, SSA determines whether to provide notice of the loss or credit monitoring to individuals potentially affected by the loss or notice of the loss to the public at large. For losses the component determines the risk of harm is moderate, high, or major, the component submits the risk assessment to SSA's OPD for evaluation and agreement on the appropriate mitigation steps.[9]

Referring Losses to the Office of the Inspector General

According to SSA's 2017 *Breach Response Plan*, the loss reporting tool automatically sent loss reports categorized as moderate, high, or major to the OIG. Additionally, SSA managers were required to report to the OIG the loss of:

1. PII of Individuals of Extraordinary National Prominence;[10]

2. any correspondence containing PII from an SSA facility that was addressed to members of the public or Agency employees before it was accepted by the U.S. Postal Service;

---

[5] SSA, *Breach Response Plan*, sec. 6, p. 7 (June 2017).

[6] SSA, *Breach Response Plan*, sec. 6, p. 7 (June 2017). On September 30, 2024, SSA's National Network Service Center rebranded as the Enterprise-IT Customer Service Desk. For consistency, we refer to this office as the service center throughout this document. SSA advised they created a new process, beginning February 2024, in which the service center inputs the loss report into SSA's loss reporting tool when SSA employees call to report a PII loss.

[7] SSA, *Information Security Policy*, Version 9.7.2, sec. 3.2, pp. 41-42 (July 2025).

[8] SSA, *Breach Response Plan*, sec. 8, pp. 9-11 (June 2017).

[9] For more information on the four risk levels, see Appendix A.

[10] Individuals of Extraordinary National Prominence include individuals such as the President, the Chief Justice, the Speaker of the House of Representatives, the Commissioner of Social Security, and other selected individuals with a higher level of general public interest, such as celebrities.

3. electronic media (Universal Serial Bus drive, Compact Disc/Digital Versatile Disc) that contains PII; or

4. PII for 50 or more individuals.

The OIG investigates allegations of criminal violations and is a member of the SSA Security Response Team.[11]

Reporting Incidents to Others

The SSA Security Response Team provides incident reports to key management personnel and reports major incidents to the U.S. Computer Emergency Readiness Team.[12] Federal agencies must report details on information security incidents, including a specification of the total number of losses, and a description of each major incident, annually to the Office of Management and Budget.[13]

SCOPE AND METHODOLOGY

We identified 2 sampling frames from a total of 27,180 PII loss reports from Calendar Years 2019 to 2023

- Sampling Frame 1 comprised 658 loss reports that were not included in SSA's legacy loss reporting tool. We reviewed a random sample of 50 of the 658 loss reports to determine whether SSA reported losses to OIG when required.

- Sampling Frame 2 comprised 26,522 reports that were included in SSA's legacy loss reporting tool. Of the 26,522 reports, 23,945 had a low-risk level, 7 had a moderate-risk level, 2 had a high-risk level, and 2,568 had a pending risk level.

    - We reviewed 70 loss reports from Sampling Frame 2 to determine whether SSA assigned the appropriate risk level and reported losses to OIG when required. Specifically, we reviewed

        - a random sample of 50 loss reports assessed as low-risk;
        - all 7 loss reports assessed as moderate-risk;
        - both loss reports assessed as high-risk; and
        - a random sample of 11 pending loss reports.

See Appendix B for more information on our scope and methodology and Appendix C for our sampling methodology and results.

---

[11] SSA, *Information Security Policy*, Version 9.7.2, sec. 3.4.8, p. 65 (July 2025).

[12] SSA, *Information Security Policy*, Version 9.7.2, sec. 4.1.3, p. 77 (July 2025).

[13] OMB, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, M-24-04, sec. VII, pp. 11-12 (December 4, 2023).

RESULTS OF REVIEW

SSA employees reported 23,954 (88 percent) of the PII losses from Calendar Years 2019 to 2023 in the legacy loss reporting tool with an assessed risk level as required. However, employees did not properly record 658 PII losses (2 percent) in the legacy loss reporting tool or assign a risk level to another 2,568 open loss reports (10 percent).[14] On average, these open loss reports remained pending for 657 days. Additionally, of the 120 loss reports we reviewed, SSA referred 4 (3 percent) to the OIG as required and did not refer 32 (27 percent) as required. (The remaining loss reports did not need to be referred to OIG.)

Loss Reporting Tool Use

SSA employees did not record 658 PII loss reports in the legacy loss reporting tool. The employees reported losses to the service center while the legacy loss reporting tool was unavailable but did not add the losses to the legacy loss reporting tool when it became available. We were unable to determine why employees did not add the losses to the legacy loss reporting tool when it became available.

Because employees did not report losses in the legacy loss reporting tool, SSA could not take appropriate actions on the loss reports. Specifically, individuals or the public at large (in the event of a major loss) would not receive the appropriate notice of the loss and would be unable to take actions such as obtaining credit monitoring or using multi-factor authentication to protect themselves from identity theft. Additionally, none of the losses could be evaluated to determine whether they should have been reported to OIG or the Office of Management and Budget. Therefore, these parties could not take necessary actions, such as OIG's Office of Investigations determining whether fraud occurred.

Beginning February 2024, employees in the service center input the loss reports into the loss reporting tool when the tool is unavailable (rather than the employees reporting the losses).

Open Personally Identifiable Information Loss Reports

As of October 21, 2024, SSA had 2,568 open PII losses with no assessed risk level. These losses were as old as January 2019 and were pending for an average of 657 days. This occurred because, although the 2017 *Breach Response Plan* stated low-risk losses should be closed in the loss reporting tool, it did not establish criteria or a time frame for closing moderate, high, or major loss reports.[15] SSA advised the pending reports from the Office of Operations constituted most of the pending loss reports and were due to a malfunction in the legacy loss reporting tool as well as Operations staffing challenges.

SSA advised the Office of Operations and OPD resolved and cleared these pending reports in the legacy version of the loss reporting tool. No loss reports were pending in the legacy loss reporting tool as of August 2025.

---

[14] Rounded up to 10 percent for the total to sum to 100 percent.

[15] SSA, *Breach Response Plan*, sec. 6, p. 8 (June 2017).

SSA did not know whether actions were needed to remediate the 2,568 PII losses while they remained open. Therefore, individuals who were affected may have been unaware that they needed to take actions, such as obtaining credit monitoring or using multi-factor authorization, to protect themselves from identity theft. The *Breach Response Plan* also noted the potential for economic or medical identity theft, reputational harm, emotional harm, financial loss, unfairness, and risk to personal safety.[16]

Risk of Harm Assessment

SSA employees reported 23,954 of the PII losses from Calendar Years 2019 to 2023 in the legacy loss reporting tool with an assessed risk level as required. Of the 70 loss reports we reviewed from Sampling Frame 2, SSA employees correctly recorded 1 loss as moderate and 50 as low. However, employees recorded eight losses as moderate or high risk that did not meet the criteria for those risk levels. Employees should have recorded these losses as low risk. Employees did not assign a risk level to the remaining 11 loss reports.

Employees reporting a PII loss were required to document an initial risk of harm assessment in the legacy loss reporting tool. Employees initially made the wrong determinations for the eight losses and, once those errors were identified, the legacy loss reporting tool did not allow employees to correct the determinations. SSA advised that employees incorrectly assessed two of these losses because they were in training and new to the PII workload.[17] Although employees incorrectly recorded the initial assessment for the eight losses in the legacy loss reporting tool, for seven of the losses, subsequent entries indicated the final assessment was low. The remaining report continued to have an incorrect final assessment. The legacy loss reporting tool did not allow changes and corrections to initial assessments. SSA's OPD advised the new loss reporting tool automatically assigns a risk level once an employee documents the loss in the tool. Component breach response coordinators and OPD can make changes and corrections to initial risk assessments in the new loss reporting tool.

When employees do not assign loss reports a risk level, individuals affected by a PII loss cannot protect themselves from potential harm, including physical, psychological or economic injury or damage, embarrassment, inconvenience, reputational harm, financial loss, unfairness or risk to personal safety.[18] Additionally, when employees assign loss reports an inappropriately high risk level, SSA unnecessarily expends resources determining whether to take actions such as sending notices, offering credit monitoring, and fielding questions about the losses.

---

[16] SSA, *Breach Response Plan*, sec. 5, p. 5 (June 2017).

[17] Employees in SSA's OPD advised they developed training and additional resources for breach response coordinators on areas including determining the risk assessment and held the training in August 2025.

[18] SSA, *Breach Response Plan*, sec. 5, p. 5 (June 2017). SSA's OPD managers advised us they established the Breach Division in November 2023. The Breach Division staff implemented a daily review process for loss reports as an oversight tool. For example, the analysts review the loss reports to identify reports that could require immediate action or executive awareness.

Referrals to the Office of the Inspector General

SSA did not refer 32 of 120 loss reports to OIG as required, including:

- 25 of 50 loss reports from Sampling Frame 1; and[19]
- 7 of 70 loss reports from Sampling Frame 2.[20]

Managers did not refer 29 loss reports with low or pending risk levels to OIG. We could not determine why managers did not refer them as policy required.

The legacy loss reporting tool did not automatically report three loss reports with moderate or high risk levels to OIG. While SSA personnel acknowledged the system did not perform as it should have in these instances, they did not explain why the system failed.[21]

SSA could improve it policies by the updating the *Breach Response Plan* to clearly explain the types of losses that managers should refer to OIG. When the appropriate loss reports are not referred to OIG, OIG is unable to determine whether they need to investigate or take additional actions.

CONCLUSION

The Agency needs to update its guidance and evaluate the effectiveness of its updated processes and controls to ensure employees respond to PII losses properly. By appropriately reporting, assessing, and referring suspected or confirmed PII losses, employees can help mitigate the potential harm to individuals and the Agency.

RECOMMENDATIONS

We recommend SSA:

1. Distribute the 658 PII losses in Sampling Frame 1 to the appropriate component(s) for review to determine whether any losses are moderate, high, or major, and, if so, identify and take the proper actions to mitigate those losses.
2. To prevent future employee errors related to reporting, assessing, and closing PII losses, evaluate the effectiveness of the processes and controls implemented by OPD and implement changes as needed.
3. Update the *Breach Response Plan* to clearly explain all actions relevant to OIG referrals, such as when managers should use forms related to lost or stolen equipment.

---

[19] The other 25 loss reports from Sampling Frame 1 did not need to be referred to OIG.

[20] Four loss reports from Sampling Frame 2 were referred to OIG as required. The remaining 59 did not need to be referred to OIG.

[21] As of July 3, 2025, OIG's Office of Investigations confirmed with SSA's OPD that the automatic referrals in the loss reporting tool appeared to be working correctly.

AGENCY COMMENTS

SSA agreed to implement our recommendations; see Appendix D.

APPENDICES

Appendix A – Breach Response Plan Risk Levels

Social Security Administration employees conduct a risk of harm assessment to categorize personally identifiable information (PII) losses into four risk levels.[1] The four risk levels range from the least severe (low) to the most severe (major), depending on the sensitivity of the PII, the number of individuals whose PII is involved, and the harm that may result or has resulted from the unauthorized, illegal, unethical disclosure of, modification, use or disposal of the information. Specifically, the risk levels are as follows.

- Low: The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets or individuals.

- Moderate: The loss of confidentiality, integrity, or availability is expected to severely affect organizational operations, organizational assets, or individuals.

- High: The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- Major: PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to national-security interests, foreign relations, or the U.S. economy or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a major incident.

[1] SSA, *Breach Response Plan*, sec. 5, p. 5 (June 2017). All of the information in this Appendix is from Section 5 of SSA's 2017 *Breach Response Plan*.

Appendix B – SCOPE AND METHODOLOGY

To meet our objective, we:

- Reviewed applicable Federal laws including sections of the *Social Security Act* and Social Security Administration (SSA) regulations, policies, and procedures.
- Reviewed prior *Federal Information Security Modernization Act* reports and recommendations regarding personally identifiable information (PII) protection.
- Compared SSA's PII protections to other Federal agencies, best practices, and requirements.
- Interviewed employees and managers to identify any control weaknesses in PII protection and the PII loss reporting or escalation process.
- Obtained PII loss reports from SSA for Calendar Years 2019 through 2023 and identified a population of 27,180 PII loss reports. We (1) compared the data with loss reports provided by the Office of Inspector General's (OIG) Office of Investigations, (2) reviewed data fields to determine whether the fields contained logical information, and (3) verified such data fields as the date range matched our requested information. We concluded the data were sufficiently reliable given the audit objective and intended use of the data.
- Identified and reviewed the following from the population of 27,180 loss reports.
    - Sampling Frame 1 comprised 658 loss reports not included in SSA's legacy loss reporting tool. We reviewed a random sample of 50 of the 658 loss reports to determine whether SSA reported losses to OIG when required.
    - Sampling Frame 2 comprised 26,522 reports included in SSA's legacy loss reporting tool. Of the 26,522 reports, 23,945 had a low risk level, 7 had a moderate risk level, 2 had a high risk level, and 2,568 had a pending risk level.
        - We reviewed 70 loss reports from Sampling Frame 2 to determine whether SSA assigned the appropriate risk level and reported losses to OIG when required. Specifically, we reviewed:
            - a random sample of 50 loss reports assessed as low-risk;
            - all 7 loss reports assessed as moderate-risk;
            - both loss reports assessed as high-risk; and
            - a random sample of 11 pending loss reports.
- Analyzed the sampled loss reports by reviewing information from SSA's legacy loss reporting tool and OIG's Office of Investigations.
- Assessed SSA's overall controls over PII loss report tracking and resolution.

The principal entity audited entity was the Office of the Chief Information Officer. We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. In addition, we reviewed the principles of internal controls associated with the audit objective. We identified the following components and principles as significant to the audit objective.

- Component risk assessment
    - Principle 6: Define objectives and risk tolerances
    - Principle 7: Identify, analyze, and respond to risks
- Component control activities
    - Principle 10: Design control activities
- Component information and communication
    - Principle 13: Use quality information
    - Principle14: Communicate internally
- Component monitoring
    - Principle 16: Perform monitoring activities
    - Principle 17: Evaluate issues and remediate deficiencies

We conducted our review between October 2024 and July 2025. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix C – Sampling Methodology and Results

We identified 2 sampling frames from 27,180 personally identifiable information loss reports from Calendar Years 2019 to 2023.

- Sampling Frame 1 comprised 658 loss reports that were not included in the Social Security Administration's (SSA) legacy loss reporting tool. We reviewed a random sample of 50 of the 658 loss reports to determine whether losses were reported to the Office of the Inspector General (OIG) when required, see Table C- 1.

Table C- 1: Sampling Frame 1 and Sample Size

Description	Number of Loss Reports
Sampling Frame	658
Sample Size	50

- Sampling Frame 2 comprised 26,522 loss reports included in SSA's legacy loss reporting tool. Of the 26,522 reports, 23,945 had a low risk level, 7 had a moderate risk level, 2 had a high risk level, and 2,568 had a pending risk level.
    - We reviewed 70 loss reports from Sampling Frame 2 to determine whether losses were assigned the appropriate risk level and reported to OIG when required, see Table C- 2.

Table C- 2: Sampling Frame 2 and Sample Size

Description	Population Size	Sample Size
Low risk loss reports	23,945	50
Moderate risk loss reports	7	7
High risk loss reports	2	2
Pending risk assessment loss reports	2,568	11
Sampling Frame	**26,522**	**70**

To conduct this review, we used a stratified random sample statistical approach. This is a standard statistical approach used for creating samples from a sampling frame that has been divided into strata. We then selected proportionate samples from each stratum completely at random. As a result, each sample item had an equal chance of being selected throughout the sampling process, and the selection of one item had no impact on the selection of other items. Therefore, we chose a sample that represented the sampling frame, absent human biases, and ensured statistically valid conclusions of the entire population under review.

Appendix D – AGENCY COMMENTS

SOCIAL SECURITY
Office of the Commissioner

MEMORANDUM

Date: September 12, 2025 Refer To: TQA-1

To: Michelle L. Anderson
Acting Inspector General

From: Chad Poist
Chief of Staff

Subject: Office of the Inspector General Draft Report, "Personally Identifiable Information Loss Reporting" (042401) -- INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Please let me know if I can be of further assistance. You may direct staff inquiries to Amy Gao at (410) 966-1711.

Mission: The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report: Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect: OIG.SSA.GOV

Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

@TheSSAOIG

OIGSSA

TheSSAOIG

Subscribe to email updates on our website.