OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Claims-taking Systems Access Profiles

A-14-17-50096 | February 2018

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: February 5, 2018 Refer To:

To: The Commissioner

From: Acting Inspector General

Subject: Claims-taking Systems Access Profiles (A-14-17-50096)

The attached final report presents the results of the Office of Audit's review. The objectives were to determine whether the Social Security Administration (1) assigned its claims-taking profiles only to users who needed them to perform their duties and (2) properly limited the resources in those profiles.

If you wish to discuss the final report, please call me or have your staff contact Rona Lawson, Assistant Inspector General for Audit, 410-965-9700.

Gale Stallworth Stone

Gale Stallworth Stone

Attachment

cc:
General Counsel

Claims-taking Systems Access Profiles
A-14-17-50096

SOCIAL SECURITY ADMINISTRATION
OIG

February 2018 **Office of Audit Report Summary**

Objectives

To determine whether the Social Security Administration (SSA) (1) assigned its claims-taking (CT) profiles only to users who needed them to perform their duties and (2) properly limited the resources included in those profiles.

Background

In Fiscal Year 2017, SSA paid nearly $1 trillion in benefits. The Agency's claims-takers played a key role in administering these benefits by reviewing and authorizing claims. Of the Agency's nearly 60,000 employees, almost 20,000 rely on SSA's information technology systems to take claims for Social Security benefits.

The Agency requires that managers authorize employee access to SSA information systems based on need to know and limit access to the least privilege required to perform job functions. SSA uses system profiles to separate duties among its users.

Each profile contains permissions to access such system resources as software applications, data files, and transactions. Based on users' job duties, SSA assigns one or more profiles to their personal identification numbers. Users can then access the system resources included in their assigned profile(s).

Findings

SSA generally assigned its CT profiles only to users who needed them to perform their duties. However, we found SSA did not maintain a list of incompatible duties for claims-takers. In addition, SSA could further limit the (1) assignment of CT profiles to only those users who needed them to perform their duties and (2) resource permissions in its CT systems access profiles.

Recommendations

We recommend SSA:

1. Document incompatible CT duties and provide detailed guidance to ensure staff considers these conflicts when assigning or changing CT profiles.
2. Confirm the need for profile assignments of those who had not used a CT profile in longer than 1 year.
3. Review the list of non-CT positions for which CT profiles had been assigned and remove the assignments from users when they conflict with the principles of least privilege, need to know, and/or separation of duties.
4. Review the list of eight personal identification numbers that have at least five additional profiles to determine the appropriateness of the assignments.
5. Remove the 29 resource permissions in its CT profiles that have not been used in over 1,095 days.
6. Ensure the Agency's automated resource permission removal tool is operating properly.
7. Determine whether it would be appropriate to remove resource permissions before 1,095 days of nonuse.
8. Explore the feasibility of implementing a control that identifies non-use of resource types excluded from the Agency's automated resource permission removal tool and removes the resource permissions whose non-use exceeds management's threshold.

The Agency agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

CT	Claims-taking
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
PIN	Personal Identification Number
SSA	Social Security Administration

OBJECTIVES

Our objectives were to determine whether the Social Security Administration (SSA) (1) assigned its claims-taking (CT) profiles only to users who needed them to perform their duties and (2) properly limited the resources in those profiles.

BACKGROUND

In Fiscal Year (FY) 2017, SSA paid nearly $1 trillion in benefits. The Agency's claims-takers played a key role in administering these benefits by reviewing and authorizing claims. Of the Agency's nearly 60,000 employees, almost 20,000 rely on SSA's information technology systems to take claims for Social Security benefits.

Access Control Requirements

SSA developed the Access Control section of its Information Security Policy to meet numerous control standards, including, but not limited to, Office of Management and Budget Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication 800-53.[1] Circular A-130 requires that agencies implement specific measures to safeguard Federal information and information systems including policies of least privilege and separation of duties as well as those that ensure appropriate authorization and need for information resources.[2] NIST Special Publication 800-53 provides security controls to help agencies comply with these and other Federal requirements.[3]

SSA policy requires that effective technical, operational, and management controls be implemented to prevent, determine, and detect improper payments and disclosures.[4] This includes controls to restrict access to Agency systems.[5] The Agency requires that managers authorize employee access to SSA information systems based on a need to know and limited to the least privilege required to perform job functions.[6] SSA policy requires that responsible

---

[1] SSA, *Information Security Policy, Version 7.7*, *Section II: Access Control*, secs. 2.1.1 Background and 2.6 References (November 30, 2017).

[2] OMB, Circular No. A-130, *Managing Information as a Strategic Resource*, Appendix I, 4. Specific Requirements, secs. i.2, 3, and 5 (July 28, 2016).

[3] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, vol. Revision 4, Information Security Due Diligence, p. x (April 2013).

[4] SSA, *Information Security Policy, Version 7.7*, *Section IV: Information Security Risk Management*, sec. Purpose (November 30, 2017).

[5] SSA, *Information Security Policy, Version 7.7*, *Separation of Duties*, sec. 4.4.2.1.13 (November 30, 2017).

[6] SSA, *Information Security Policy, Version 7.7*, *Access Management*, sec. 2.1.6 (November 30, 2017).

personnel limit access to those who have a legitimate need for these resources to perform their assigned position responsibilities.[7]

One access control technique SSA uses to protect information systems is separation of duties[8] whereby an organization divides roles and responsibilities so a single individual cannot subvert a critical process.[9] After system owners evaluate their business process for risks, they can choose from a number of possible solutions to implement separation of duties controls.[10]

Access Control Processes

SSA uses system profiles to separate duties among its system users. Each profile contains permissions to access such system resources as software applications, data files, and transactions. Based on job duties, the Agency assigns one or more profiles to users' personal identification numbers (PIN). Users can then access the system resources in their assigned profile(s).

SSA has various controls in place to ensure appropriate profiles and contents are assigned. For example, the Agency has processes and system tools for authorizing profile assignments and conducting recurring reviews of those assignments. The Agency also has processes and tools to review the resource permissions included in its profiles and remove permissions from profiles when they have not been used in over 1,095 days.

Separating duties may not always be cost-effective. When SSA converted the manual CT system to the forerunner of the current automated systems, SSA determined it would be more efficient to allow one employee to perform the four key CT functions instead of continuing to separate those functions.[11] The Agency implemented compensating controls (for example, automated integrity reviews) to mitigate this lack of operational separation of duties.[12] SSA's policy still requires that compensating controls be used to mitigate any lack of operational separation of duties.[13]

---

[7] SSA, *Information Security Policy*, *Version 7.7*, *Access Management*, sec. 2.1.6 (November 30, 2017).

[8] SSA, *Information Security Policy*, *Version 7.7*, *2.1 Information Systems Logical Access Control Policy*, sec. 2.5 Definitions (November 30, 2017).

[9] SSA, *Information Security Policy*, *Version 7.7*, *2.1 Information Systems Logical Access Control Policy*, sec. 2.5 Definitions (November 30, 2017).

[10] SSA, *Information Security Policy*, *Version 7.7*, *Separation of Duties*, sec. 4.4.2.1.13 (November 30, 2017).

[11] The four key functions are creating a claim, modifying a claim, entering a claim award or denial decision, and submitting a claim for further processing. Department of Health and Human Services, Office of Inspector General, *Separation of Duties in the Social Security Administration's Modernized Claims System, A-13-89-00025*, pp. 1 and 4 (February 8, 1990).

[12] Department of Health and Human Services, Office of Inspector General, *Separation of Duties in the Social Security Administration's Modernized Claims System, A-13-89-00025*, pp. 5-6 (February 8, 1990).

[13] SSA, *Information Security Policy*, *Version 7.7*, *Integrity Review Process*, sec. 4.4.2.1.11 (November 30, 2017).

Through discussions with the Agency, we identified 10 profiles that SSA could assign to CT staff to enable them to process claims. To conduct our review, we analyzed all 10 of these profiles. We used data from SSA's eTrust tool[14] to determine how many users had access to CT profiles, the number of days since they last accessed their CT profiles, and the number of days since each resource in the CT profiles had been accessed.[15] See Appendix A for more on our methodology.

RESULTS OF REVIEW

SSA generally assigned its CT profiles only to users who needed them to perform their duties. However, we noted that SSA did not maintain a list of incompatible duties for claims-takers, which increased the risk of providing access that conflicted with the principle of separation of duties. In addition, we identified instances where SSA could further limit the assignment of CT profiles. Specifically, some employees had not used their assigned CT profile(s), staff in non-CT positions had been assigned CT profiles, and staff had been assigned multiple profiles.

In addition, we found that SSA could better limit the resource permissions in its CT profiles. Individuals had not used many resource permissions, indicating they may not have needed them. Further, SSA's automated tool to remove unused resource permissions had not operated as intended. We identified 29 resource permissions that met the removal threshold but had not been removed by the tool.

Incompatible Duties for Claims-takers

Although SSA staff provided examples of CT actions it separates, we were unable to obtain a comprehensive list of incompatible duties for claims-takers or a risk analysis of CT duties. Without a list of incompatible duties, we believe SSA managers and security officers may not have a sufficient basis to prevent separation of duties conflicts when authorizing profile assignments or when adding resource permissions to profiles. For example, authorizing individuals may not be aware that assigning a profile to a user conflicts with a profile already assigned to that user. In addition, without identifying incompatible duties, the Agency cannot ensure it has comprehensively addressed CT risks.

[14] The eTrust tool report shows the last date of access for each PIN that can access a profile and for each resource assigned to a profile. The eTrust data used for our analysis was obtained on different days during the first week of June 2017. SSA extracted: (1) an eTrust report for one CT profile on June 2; (2) reports for four CT profiles on June 5; and (3) reports for five CT profiles on June 7, 2017.

[15] SSA has roughly 60,000 employees. We found that 19,741 of its systems users had access to at least 1 of the 10 profiles in June 2017.

SSA uses profiles to limit systems access while supporting separation of duties. According to NIST, implementing separation of duties requires that organizations define the duties of individuals or roles, document the duties to be separated, and define authorized information systems access to support the separated duties.[16]

Given SSA's high number of CT staff and their role in authorizing benefits, we believe it is essential for the Agency to ensure it identifies and addresses risks caused by incompatible duties. Therefore, we recommend that SSA document incompatible CT duties and provide detailed guidance to ensure staff considers these conflicts when assigning or changing CT profiles.

Limiting the Assignment of CT Profiles

To ensure adherence to the principles of least privilege access and need to know, SSA requires that every user's profile assignments be reviewed and certified at least once every 3 years.[17] Despite this process, we identified Agency personnel assigned profiles they did not appear to need to perform their duties.

Not Actively Using Assigned CT Profile(s)

Based on SSA eTrust data from the first week of June 2017, 19,741 users had access to at least 1 CT profile.[18] These data also indicated the number of days since these individuals had last used their assigned CT profile. Specifically, 334 had not used their CT profile in at least 30 days. Of those 334, 89 and 33 had not used their profile in longer than 365 days and 1,095 days, respectively. Table 1 shows an aging analysis of the 334 instances where an assigned CT profile had not been used in longer than 30 days.

Table 1: Days of CT Profile Non-use Longer than 30 Days (as of Early June 2017)

Days Unused	31-90	91-180	181-365	366-730	731-1,095	Over 1,095	Total
Number of CT Profile Assignments Used at Least Once	124	64	57	30	11	6	292
Number of CT Profile Assignments Never Used	0	0	0	12	3	27	42
Total	**124**	**64**	**57**	**42**	**14**	**33**	**334**

[16] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, Appendix F, Security Control Catalog, sec. AC-5 Separation of Duties (April 2013).

[17] SSA, *Information Security Policy, Version 7.7, Section II: Access Control*, secs. 2.4 Roles and Responsibilities and 2.1.6 Access Management (November 17, 2017). SSA reviews all employees triennially. However, certain groups of users, such as contractors and new hires, are reviewed annually.

[18] These 19,741 users had access to 19,957 CT profiles because 216 users had access to 2 CT profiles.

Table 2 identifies the positions of the 89 individuals who had not used their assigned CT profile in over 365 days of the eTrust data we obtained. Of the 89, 47 had used their CT profile at least once, while 42 had never used their CT profile. Although we concluded from the position names that many were claims-takers, it appeared these individuals did not require their CT profile assignment to perform their duties.

Table 2: Positions Associated with CT Profiles Not Used in Longer than 1 Year (as of Early June 2017)

SSA Position Title	CT Profile Used At Least Once	CT Profile Never Used	Total
Claims Specialist	34	24	58
Claims Technical Expert	4	6	10
Foreign Service Post Staff	1	2	3
Operations Supervisor	0	3	3
Mail Clerk	1	1	2
Unknown[19]	5	3	8
Other[20]	2	3	5
Total	**47**	**42**	**89**

SSA stated it considered implementing a process to automatically remove unused profile assignments. However, the Agency found that, in certain instances, its systems might incorrectly indicate profile non-use. Therefore, automatically removing profiles that appear to be unused could prevent staff from performing their job duties. Nevertheless, to ensure the Agency limits access to the least privilege required for performing job function, we recommend that SSA confirm the need for these profile assignments.

Non-CT Positions Assigned CT Profiles

We identified instances where individuals who did not appear to be in CT positions had CT profiles assigned and had used these profiles within 30 days of our testing. Table 3 includes examples of these positions, the total number of SSA employees in each position number, and those who used the CT profile within 30 days of the eTrust data.

[19] The human resources data we obtained did not contain a record for these eight individuals as of June 6, 2017, and the individuals did not have an email record.

[20] We identified five additional positions where an individual had either used the profile at least once but had not used it since or had never used it for over 1 year.

Table 3: Examples of Non-CT Positions Using CT Profiles Within the Last 30 Days (as of Early June 2017)

SSA Position Title	Position Number[21]	Total Number of SSA Employees[22]	Used CT Profile Within 30 Days
Public Affairs Specialists	05D0760, 08B4180, 091Q840, 094I020, 095T300, 096H610, 096L590, 097J550, 098K230, 098K650, 099Q810	95	42
Management Support Specialists	06C0750	191	32
Systems Coordinators	05E3250	250	27
Intake & Scanning Clerks	039B740, 095U110	20	16
Technical Training Instructors	04D0510	25	15
Human Resources Specialists	01D0630	15	5
Regional Security & Integrity Specialists	08C0070	31	5
Reader Assistants	08C0860, 08C0870	126	5
Administrative Assistants	039B830	12	4
District Office Administrative Assistants	04D0860	173	4
Console Operator	04B1110	17	4
Audio Visual Production Specialists	09E6950	9	3
Interactive Video Teletraining Studio Technician	08B1650, 08B165A	14	3
Staff Assistant	03E5110, 08B4050	52	2
Regional Communications Director	00D049S	9	2
Mail Clerk	0374770	5	1

Users who have access to a CT profile who are not CTs may possess a greater level of access than required to perform their duties. Additionally, their use of a CT profile may allow improper activity. Therefore, we recommend that SSA review the list of non-CT positions for which CT profiles have been assigned and remove the assignments from users when they conflict with least privilege, need to know, and/or separation of duties principles.[23]

[21] The Position Number column in Table 3 includes only the position numbers for which an individual was assigned a CT profile. The Total Number of SSA Employees column reflects the total number of Agency staff with the identified position numbers. However, position titles may be associated with additional position numbers that are not reflected in the Table.

[22] See Footnote 21.

[23] We will separately provide SSA with the list of individuals assigned a CT profile and their respective positions.

Multiple Profiles in Addition to CT Profiles

Between April and June 2017, we obtained lists that identified all profiles assigned to SSA system users who had a CT profile.[24] Of the 19,583 users, 18,905 had CT positions and 678 did not. After removing known administrative profiles[25] and profiles used for training or testing, 13,689 users did not have profiles assigned beyond their CT profile. However, 35 users had at least 5 additional profiles. Table 4 shows the number of non-CT profiles assigned to users with CT profiles.[26]

Table 4: Number of non-CT Profiles Assigned to Users with CT Profiles

Number of Non-CT Profiles	0	1	2	3	4	5 to 10	11 to 14	Total
CT Position	13,357	4,417	888	185	48	10	0	18,905
Non-CT Position	332	221	52	27	21	24	1	678
Total	**13,689**	**4,638**	**940**	**212**	**69**	**34**	**1**	**19,583**

We obtained the names of the profiles assigned to the 35 users who had at least 5 non-CT profiles assigned to their PINs. Upon further review, 27 of the 35 had fewer than 5 additional profiles after discounting profiles that granted access to such applications as badging and union time monitoring activities. Of the eight with five or more additional profiles, one had a CT position and seven did not. One of the users with a non-CT position was a systems analyst who had 14 additional profiles.

Assigning many profiles to a single user could negate the separation of duties implemented through profile use. Given the high number of profile assignments compared to the total population and the potential impact to separation of duties, we recommend SSA review the list of the eight PINs with five or more non-CT profiles to determine the appropriateness of the assignments relative to separation of duties, least privilege access, and need to know principles.

[24] These lists included records for 19,583 of the 19,741 users identified by eTrust.

[25] Administrative profiles related to managerial functions include payroll, performance assessment, and security.

[26] We obtained profile assignment data between April and June 2017 (April 28, April 30, May 1, and June 30).

Resource Permissions in CT Profiles

SSA has processes in place to ensure profiles contain appropriate permissions to system resources. For example, the Agency makes reports that indicate when resources were last used available to those responsible for maintaining profiles.[27] In addition, SSA periodically reviews and certifies the resource permissions in profiles. In FY 2013, the Agency last reviewed and certified the contents of the 10 CT profiles that could be assigned to employees for processing claims. Despite these processes, many resource permissions in CT profiles had not been used and therefore may not have been required.

Using SSA's eTrust records from early June 2017, we created an aging table to show instances of unused resource permissions in the 10 CT profiles. As shown in Table 5, between 14 and 88 percent of the resources in each CT profile had not been used in over 365 days.[28] Of the 3,499 instances of resources that had not been used in over 365 days, 482 (14 percent) had never been used.[29]

Table 5: Instances of Unused Resource Permissions in CT Profiles (as of Early June 2017)

CT Profile	Days Unused								Unused in over 365 Days	
	0-30	31-90	91-180	181-365	366-730	731-1,129	Over 1,129	Total		
1	1,394	107	36	40	261	61	3	1,902	325	17%
2	1,118	149	85	79	277	88	3	1,799	368	20%
3	1,723	86	17	13	278	36	3	2,156	317	15%
4	84	14	6	17	678	178	9	986	865	88%
5	607	134	43	56	265	254	2	1,361	521	38%
6	381	88	47	24	125	64	1	730	190	26%
7	311	38	28	26	111	55	2	571	168	29%
8	765	65	29	31	160	47	3	1,100	210	19%
9	1,338	131	44	43	239	64	3	1,862	306	16%
10	1,076	128	53	179	166	63	0	1,665	229	14%
Totals	8,797	940	388	508	2,560	910	29	14,132	3,499	25%
Never Used[30]	**2**	**4**	**7**	**162**	**147**	**309**	**26**	**657**	**482**	**73%**

[27] SSA does not require review of these reports.

[28] Table 5 does not include 1,746 eTrust records for the EJBRole resource type, for which usage data may not be accurate. EJBRoles limit access within applications that use the JAVA programming language.

[29] The 10 CT profiles contain many of the same resource permissions since each profile supports SSA's CT process. At the time of our analysis, the 10 profiles contained 2,727 unique resource permissions.

[30] As of the first week in June 2017, 657 resource permissions had been added to CT profiles over time, but were never used after they were added.

According to SSA, resource permissions may go unused because

- business cycles may not require that users regularly access certain resources, and
- profiles may contain permissions for resources the Agency no longer uses.

However, resource permissions that remain unused for a long time may conflict with the least privilege principle and could provide the opportunity for improper activity.

Automated Removal of Resource Permissions

To ensure profiles do not contain unnecessary resource permissions, SSA developed an automated solution to identify, track, and remove resource permissions from profiles that have gone unused for longer than 1,095 days. Because this is a monthly process, it could take SSA 1,129 days to remove a record.

SSA data indicated that, between June 2016 and May 2017, its automated tool removed 722 resource permissions from the 10 CT profiles we reviewed. We verified the 10 CT profiles no longer contained any of these 722 resource permissions. However, we identified 29 other resource permissions within CT profiles that had not been used in longer than 1,129 days and had not been removed by the tool. We recommend SSA remove these resources and ensure its automated tool is functioning properly. SSA may also want to determine whether it would be appropriate to remove resource permissions before 1,095 days of nonuse.

In addition, the automated solution excludes one type of resource permission because of unreliable usage data.[31] The Agency stated that removing these permissions could keep users from performing their job duties. However, SSA expects to continue increasing its use of this particular resource type as it modernizes its systems. Therefore, controls over this type of resource will become increasingly important. As a result, we recommend the Agency explore the feasibility of implementing a control that identifies non-use of this resource type and removes the resource permissions whose non-use exceeds management's threshold.

CONCLUSIONS

SSA maintains sensitive data on nearly every U.S. citizen and pays approximately $80 billion in benefits each month. Therefore, it is critical the Agency properly limit access to the systems that store and process its data. SSA has many controls in place to ensure it provisions system access based on the principles of least privilege and need to know. However, we found SSA did not maintain a list of incompatible duties for claims-takers, which limited management's ability to prevent separation of duties conflicts. Further, SSA had not always (1) limited the assignment of CT profiles to only those users who need them to perform their duties or (2) properly limited the resources included in its CT profiles. While SSA had made a concerted effort to limit systems access and mitigate risks, it should continue improving its processes to prevent possible misuse.

[31] The automated solution does not remove EJBRole resources. See Footnote 28.

RECOMMENDATIONS

We recommend SSA:

1. Document incompatible CT duties and provide detailed guidance to ensure staff considers these conflicts when assigning or changing CT profiles.

2. Confirm the need for profile assignments of those who had not used a CT profile in longer than 1 year.

3. Review the list of non-CT positions for which CT profiles had been assigned and remove the assignments from users when in conflict with the principles of least privilege, need to know, and/or separation of duties.

4. Review the list of eight PINs that have at least five additional profiles to determine the appropriateness of the assignments relative to the principles of separation of duties, least privilege access, and need to know.

5. Remove the 29 resource permissions in its CT profiles that have not been used in longer than 1,095 days.

6. Ensure the Agency's automated resource permission removal tool is operating properly.

7. Determine whether it would be appropriate to remove resource permissions before 1,095 days of nonuse.

8. Explore the feasibility of implementing a control that identifies non-use of resource types excluded from the Agency's automated resource permission removal tool and removes the resource permissions whose non-use exceeds management's threshold.

AGENCY COMMENTS

SSA agreed with our recommendations. The full text of SSA's comments is in Appendix B.

Rona Lawson
Assistant Inspector General for Audit

APPENDICES

Appendix A – Scope and Methodology

To accomplish our objectives, we:

- Reviewed applicable Federal laws and guidance, including the *Federal Information Security Modernization Act of 2014*,[1] Office of Management and Budget Circular A-130,[2] and National Institute of Standards and Technology Special Publication 800-53.[3]

- Reviewed the Social Security Administration's (SSA) policies and procedures pertaining to systems access.

- Met with key SSA personnel to discuss separation of duties and obtain a list of profiles used by claims-takers. Based on these discussions, we confirmed there were 10 claims-taking (CT) profiles. The 10 CT profiles are P00022P, P00023P, P00024P, P00061P, P00157P, P00173P, P00174P, P00343P, P00353P, and P00912P.

- Obtained a Human Resources database extract that contained the personal identification numbers (PIN), position names, and related information for every employee record that was active between October 1, 2015 and March 9, 2017.

- Obtained from SSA's access control software lists of all profiles assigned to the PINs that could access CT profiles between April and June 2017.

- Obtained 16,522 eTrust records from SSA's access control software between June 2 and June 7, 2017 for the 10 CT profiles, which showed the number of days since a resource was last accessed. In Table 5, we grouped 14,132 of these 16,522 records by aging categories. We excluded 1,746 records related to EJBRole resources because the eTrust information was deemed by SSA to be unreliable.[4] As such, SSA excludes the EJBRole records from its automated control to remove unused resources each month. We also excluded 644 eTrust records showing information about resources no longer assigned to the 10 CT profiles. We separately sent a list of these 644 records to SSA for review.

[1] *Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283 Stat. 3073 (2014).

[2] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

[3] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, vol. Revision 4 (April 2013).

[4] EJBRoles limit access within applications that use the JAVA programming language.

This list also contained every PIN assigned to each CT profile and the number of elapsed days since each PIN accessed each CT profile. These reports provided 19,957 PINs, of which 19,741 were unique. We found that approximately 216 PINs had been assigned more than 1 CT profile. We excluded 92 eTrust records showing information about profiles no longer assigned to users. We separately sent a list of these 92 records to SSA for review. We also excluded one record for a user whose PIN was changed.

- Obtained the last 13 months of the unused resources removal report as of June 2017.

To assess the reliability of the data we used for our analyses, we (1) performed electronic testing for obvious errors in accuracy and completeness; (2) reviewed related documentation; and (3) worked closely with Agency officials to identify any data problems. When we found discrepancies (such as unpopulated fields or data entry errors), we brought them to SSA's attention. Despite minor discrepancies, we determined that the data were sufficiently reliable for the purposes of our audit.

We conducted our audit at SSA Headquarters in Baltimore, Maryland, from January through November 2017. 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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: January 31, 2018 Refer To: S1J-3

To: Gale S. Stone
Acting Inspector General

Stephanie Hall

From: Stephanie Hall
Acting Deputy Chief of Staff

Subject: The Office of the Inspector General Draft Report, "Claims-taking Systems Access Profiles" (A-14-17-50096) -- INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "CLAIMS-TAKING SYSTEMS ACCESS PROFILES" (A-14-17-50096)

We appreciate OIG recognizing that, in general, we assigned profiles within their respective region or component to only the users who need to perform their duties. We strive to ensure that we assign profiles with the least privilege/need-to-know security principles and our separation of duties policy. While there may have been some instances of inappropriately assigned profiles, security personnel and managers work to ensure that we follow security principles and separation of duties policy. The report accurately notes that to assist in that effort, we perform triennial certification reviews and random security audits to ensure that employee access is correct, and to reduce the number of employees with access to information based on separation of duties. Below are our responses to the recommendations.

Recommendation 1

Document incompatible claims taking (CT) duties and provide detailed guidance to ensure staff considers these conflicts when assigning or changing CT profiles.

Response

We agree.

Recommendation 2

Confirm the need for profile assignments of those who had not used a CT profile in longer than 1 year.

Response

We agree.

Recommendation 3

Review the list of non-CT positions for which CT profiles had been assigned and remove the assignments from users when they conflict with the principles of least privilege, need to know, and/or separation of duties.

Response

We agree.

Recommendation 4

Review the list of eight personal identification numbers that have at least five additional profiles to determine the appropriateness of the assignments.

Response

We agree.

Recommendation 5

Remove the 29 resource permissions in its CT profiles that have not been used in over 1,095 days.

Response

We agree

Recommendation 6

Ensure the Agency's automated resource permission removal tool is operating properly.

Response

We agree.

Recommendation 7

Determine whether it would be appropriate to remove resource permissions before 1,095 days of nonuse.

Response

We agree.

Recommendation 8

Explore the feasibility of implementing a control that identifies non-use of resource types excluded from the Agency's automated resource permission removal tool and removes the resource permissions whose non-use exceeds management's threshold.

Response

We agree.

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (https://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.


Watch us on YouTube


Like us on Facebook


Follow us on Twitter


Subscribe to our RSS feeds or email updates

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at https://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at https://oig.ssa.gov/e-updates.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website:	https://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing