OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Access to Social Security Administration Data at the Disability Determination Services

A-15-11-01127| January 2013

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: January 29, 2013 Refer To:

To: The Commissioner

From: Inspector General

Subject: Access to Social Security Administration Data at the Disability Determination Services (A-15-11-01127)

The attached final report presents the results of our audit. Our objectives were to determine whether (1) security profiles assigned to disability determination services (DDS) employees provide access to Social Security Administration (SSA) data they do not need, (2) terminated DDS employees continue to have access to SSA systems, and (3) DDSs have an appropriate process for requesting and approving access to SSA systems.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

Summary of Access to Social Security Administration Data at the Disability Determination Services
A-15-11-01127

January 2013

Objective

To determine whether (1) security profiles assigned to disability determination services (DDS) employees provide access to Social Security Administration (SSA) data they do not need, (2) terminated DDS employees continue to have access to SSA systems, and (3) DDSs have an appropriate process for requesting and approving access to SSA systems.

Background

SSA's systems access policy is built on the principles of least privilege and need-to-know. Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in assuring the confidentiality, integrity, and availability of the Agency's information technology resources.

Our Findings

DDSs have a responsibility to safeguard sensitive SSA data entrusted to them to ensure SSA DDS systems are not compromised. We reviewed DDS employees' systems access at 14 DDSs nationwide. Although the Agency has controls in place to review DDS employee access, we found that DDS employees were granted unnecessary access. We noted that DDS employees were assigned profiles that were not appropriate for their job functions and profiles that had not been used for an extended period of time. We also found that there was not a consistent process among the DDSs for removing access of terminated employees. This potentially led to the untimely removal of access for several employees. By not removing separated employees' system access timely, personnel may have inappropriate access to SSA systems. DDSs should formally document the processes for obtaining and removing access to ensure procedures are followed consistently. We found that several DDSs did not have formally documented policies and procedures.

Our Recommendations

Because the issues noted above have previously been identified as part of the Fiscal Year 2011 Financial Statement Audit and are still ongoing, we recommend that the Agency strengthen various policies to ensure that systems access for DDS employees is monitored and maintained properly.

The Agency agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

C.F.R.	Code of Federal Regulations
CSI	Center for Security and Integrity
DDS	Disability Determination Services
ISSH	Information Systems Security Handbook
IT	Information Technology
ODD	Office of Disability Determinations
PIN	Personal Identification Number
POMS	Program Operations Manual System
Pub. L. No.	Public Law Number
RO	Regional Office
SSA	Social Security Administration
TEC	Triennial Certification

OBJECTIVE

Our objectives were to determine whether (1) security profiles assigned to disability determination services (DDS) employees provide access to Social Security Administration (SSA) data they do not need, (2) terminated DDS employees continue to have access to SSA systems, and (3) DDSs have an appropriate process for requesting and approving access to SSA systems.

BACKGROUND

On September 1, 1954, President Eisenhower signed into law the *Social Security* Amendments of 1954.[1] As part of the Amendments, the law sets forth the conditions for making disability determinations. The State Vocational Rehabilitation Agencies or other appropriate State agencies, under agreements with the Secretary of Health, Education, and Welfare,[2] would determine whether the individual was suffering from a disability and the days the disability began and ceased.

In June 1980, Congress passed additional legislation strengthening the disability program.[3] In passing the 1980 legislation, Congress sought to ensure effective and uniform administration of the disability programs nationwide by strengthening the Federal management of the State disability determination process. To this end, it abolished the system of individual State agreements. It also required that the Secretary of Health, Education, and Welfare promulgate regulations specifying performance standards and administrative procedures States must follow when conducting disability determinations. According to the Agency, Federal regulations[4] limit the amount of guidance Federal agencies can require of DDS' personnel selection. The regulations allow States to adhere to applicable State-approved personnel standards in the selection, tenure, and compensation of any individual employed in the disability program.

[1] Pub. L. No. 83-761, 68 Stat. 1052.

[2] Reorganization Plan No. 1 of 1953 established the Department of Health, Education, and Welfare. It was then re-designated the Department of Health and Human Services by Pub. L. No. 96-88, §509, 93 Stat.688, 695, effective May 4, 1980. Effective March 31, 1995, SSA was established as an independent agency by the *Social Security Independence and Program Improvements Act of 1994*, Pub. L. No. 103-296, § 101, 108 Stat. 1464, 1465.

[3] *Social Security Disability Amendments of 1980*, Pub. L. No. 96-265, 94 Stat. 441.

[4] 20 C.F.R. §§ 404.1621(b) and 416.1021(b).

The function of disability determinations has remained with the States since the 1954 legislation. All 50 States, plus the District of Columbia and Puerto Rico, have DDS locations. Some States have multiple sites, for a total of 116 physical locations[5] as of August 3, 2012.[6] For the week ended August 3, 2012, the DDSs had 16,143 full- and part-time employees.

To accomplish our objectives, we reviewed 14 State DDSs. These DDSs comprised approximately 52 percent of the Title II and XVI disability workloads nationwide and had approximately 7,967 full- and part-time employees[7] for the week ended August 3, 2012.

Systems Access

SSA's Systems Access Policy is contained in Chapter 2 of its Information Systems Security Handbook (ISSH). This Policy is based primarily on Office of Management and Budget Circular A-130[8] and National Institute of Standards and Technology Special Publication 800-53.[9]

SSA's systems access policy is built on the principles of least privilege[10] and need-to-know.[11] Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in assuring the confidentiality, integrity, and availability of the Agency's information technology (IT) resources.[12] This policy applies to all SSA employees and other authorized users, such as employees of other agencies, business partners, contractors, agents, and any other individuals operating on behalf of the Agency having direct access to and/or using SSA information system resources.[13]

---

[5] This figure also includes administrative offices.

[6] For purposes of this audit, we are reporting on 52 DDSs, 1 per State plus the District of Columbia and Puerto Rico, regardless of how many DDS sites a State may have.

[7] This number does not include contractors for the DDSs.

[8] Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

[9] National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

[10] The process of granting users only that access to applications and transaction screens they need to perform their official duties and of limiting their access to Agency information systems to specific applications and levels of access based on their job functions.

[11] The legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission. Approved access to Agency information systems is limited to specific applications and levels of access based on job function(s).

[12] SSA's ISSH, *Systems Access Policy*, Section 2.1, Purpose.

[13] SSA's ISSH, *Systems Access Policy*, Section 2.2, Scope.

Although the ISSH contains SSA's Systems Access Policy, the detailed policy and procedures for the DDSs are contained in SSA's Program Operations Manual System (POMS).

SSA uses Top Secret security software to provide a security access control for SSA systems. This is achieved through the use of a personal identification number (PIN) that is unique to each individual.

The profile is one of Top Secret's primary access control mechanisms. SSA develops most profiles for specific job positions (positional profiles). Each profile contains a unique mix of facilities and transactions that determines what access to systems resources each position needs. DDS staff members are also assigned functional profiles that augment selected employees' access when it is not desirable to change the positional profile.

DDS employees, management and security officers prepare Form SSA-120, *Application for Access to SSA Systems*, to request access to SSA systems. The DDS security officer then submits the Form to the Center for Security and Integrity (CSI) in its SSA region for approval. A CSI Security Officer reviews and approves the request, issues a PIN, and notifies the DDS Security Officer that the PIN has been issued.

For the DDSs in our review, the four most assigned positional profiles were Examiner, Clerical, Medical Consultant, and Single Decision Maker. All of these profiles allow individuals to search for and view disability claim information in the client's SSA electronic folder. Three of the profiles allow the ability to use the electronic case analysis tool to electronically sign/unsign disability determinations and electronically submit case records to SSA. These profiles allow access to personally identifiable information and should be monitored closely.

Prior Audit Findings

The Fiscal Year 2011 financial statement audit conducted by Grant Thornton, LLP identified logical access control weaknesses at the DDSs. Specifically, during one of the DDS site visits, Grant Thornton, LLP noted the removal of access for personnel separations was not conducted timely. Grant Thornton, LLP also noted that there were no formally documented policies and procedures regarding employees obtaining access to SSA systems. As part of this review, we conducted testing in these two areas to determine the extent of the issues.

RESULTS OF REVIEW

DDSs have a responsibility to safeguard sensitive SSA data entrusted to them and to ensure SSA and DDS systems are not compromised. We reviewed DDS employees'[14] systems access at 14 DDSs nationwide. Overall, our review determined that (1) DDS employees were granted access that was not necessary to complete their job functions, (2) the removal of terminated

[14] For this review, we included all individuals (that is, employees and contractors) with systems access at the DDS. For this report, employees will refer to both employees and contractors.

employees' access was not executed timely, and (3) DDSs did not have formally documented policies and procedures regarding employees obtaining access to SSA systems.

DDS Employees Granted Unnecessary Access

To determine whether profiles assigned to DDS employees followed SSA's policy of least privilege and need-to-know, we completed the following testing for each of the 14 DDSs.

- Compared a list of profiles provided by the Agency to all profiles assigned to all employees.
- Compared assigned profiles to the employees' job titles and descriptions for a sample of employees.
- Reviewed the number of days profiles and PINs were unused for all employees.

Based on our review, we found that profiles assigned to employees in some States were either inappropriate or not removed timely after the employees' job duties ceased. We also noted that many employees had profiles that had been unused for extensive periods and therefore we believe the access was no longer necessary.

Profiles Provided by the Agency Compared to DDS Profiles

We obtained a list of all profiles assigned to DDS employees from the Office of Disability Determinations (ODD). We compared this list to all profiles assigned to employees in the 14 DDSs to determine whether any profiles were inappropriately assigned.[15] Our comparison noted several profiles that were assigned to DDS employees but were not included in the list ODD provided. We requested explanations from the Agency to determine the appropriateness of the profiles. Based on the Agency's response, we noted the following.

- In one region, a profile was assigned to one individual as a "temporary work around"[16] and had not been removed as of the time of our comparison.
- A Top Secret error automatically assigned the Performance Assessment and Communications System profile[17] to employees.
- One user was assigned an inappropriate profile that the Agency stated had been removed.

[15] This testing was not conducted on a person-by-person basis but a review of profiles assigned overall in the 14 DDSs.

[16] A method used for achieving a task or goal when the usual or planned method isn't working.

[17] This profile was used for documenting performance assessments.

- In one region, seven users had a profile that they no longer needed and therefore was removed.

Based on the principles of least privilege and need-to-know, DDS employees should only have the access needed to complete their job functions. Additional access can lead to unauthorized entry into SSA's systems. DDS management should ensure that employee access is monitored and only the appropriate profiles are assigned.

Assigned Profiles Compared to Job Titles and Descriptions

We reviewed a sample of 630 DDS employees (45 employees from each of the 14 DDSs) to determine whether the profiles assigned appeared reasonable based on the employees' job titles and descriptions. Based on our testing we found the following.

- Three States assigned profiles to six employees that were not appropriate for their job functions.

- One State assigned both the Examiner and Clerical profiles to a secretary. The Examiner profile was assigned in error and was discovered during an internal review. The individual had both profiles inappropriately assigned for approximately 20 months before being corrected.

- One State did not remove the Examiner profile once the individual's duties as an Examiner ceased in December 2011. This error was caught and corrected in May 2012.

For one of the three States that assigned inappropriate profiles, a Systems Programmer was assigned the Clerical profile. The Clerical profile provides access to search and view disability claim information in the client's SSA Electronic Folder and copy Electronic Folder images and exhibits to a compact disc. Therefore, the Systems Programmer had access to information that was not needed to perform his/her job duties. As of October 2012, the Clerical profile had not been removed from this individual; however, the account was inactive.

For the second State, four individuals were assigned inappropriate profiles. One individual was a Data Systems Coordinator, which involved developing word processing procedures and assisting others with case processing and applications. This individual was assigned the Examiner profile, which allowed access to search and view disability claim information in the client's SSA Electronic Folder. This access was inappropriate for the individual's job duties. Another individual was a Secretary but was assigned the Medical Consultant profile. The Medical Consultant profile gave this individual access to search and view disability claim information, create initial-level disability cases, and electronically sign/un-sign disability determinations and send case records to SSA. The final two individuals were Disability Claims Supervisors but had Examiner profiles. According to the DDS, these individuals should have had the Supervisor profile. Although the main function of the Examiner profile is included in the Supervisor profile, the DDS should ensure that all individuals have the appropriate profiles.

For the third State, an Accounts Payable Contract Consultant was assigned the Case Control Supervisor profile in November 2003. This profile allowed the individual to search for and view disability claim information in the client's SSA Electronic Folder, perform a supervisory override in the Electronic Folder when the software stops a claim from being transferred, and unlock claims that were locked by users and copy Electronic Folder images and exhibits to a compact disc. According to the DDS, this profile was assigned in error, and this individual should have been given the Clerical profile. According to a Top Secret report, the Case Control Supervisor profile was not removed before the individual's employment ended in July 2011. Therefore, this employee was assigned additional access for over 7 years.

Nonuse of Profiles and PINs

Adhering to the principles of least privilege and need to know helps reduce the risk of compromising the confidentiality, integrity, or availability of SSA's IT resources. SSA uses its triennial certification (TEC) process to enforce compliance with these access control principles.

During the TEC process, managers review each of their employees' profiles and determine whether the employees have only those profiles needed to do their jobs. If the managers determine an employee no longer needs a profile, they are supposed to instruct the security officer to remove the profiles from the employees' PINs. According to the Agency, there is no specific timeframe for determining whether a profile is needed based on the amount of time it has been unused.

To examine the status of nonuse of profiles and PINs, we obtained an IT Resource Usage Report[18] as of April 15, 2011[19] from SSA's Office of Telecommunications and Systems Operations for all individuals at the 14 DDSs.[20] Since SSA did not have criteria for a number of days of nonuse in which a profile is no longer needed, we reviewed industry standards to determine a reasonable number of days of nonuse before a profile should be removed. According to industry standards,[21] ". . . disabling user accounts after 60 or 90 days of inactivity mitigates danger of unauthorized access. Stale accounts are risky—and unauthorized use of

[18] The eTrust Cleanup Report (IT Resource Usage Report) shows a profile's and PIN's last date of access. For any profile or PIN, the report lists how many days have elapsed since the date of last usage (Days Unused column).

[19] During our initial review of the report, we noted several States that had individuals missing from the report. Therefore, updated reports were requested to ensure a complete population. We obtained the updated reports for one State as of July 28, 2011 and for four States as of September 15, 2011.

[20] We reviewed 9,785 individuals with an assigned PIN at the 14 DDSs. This total can include employees as well as contractors that were assigned a PIN.

[21] NETIQ, *Sarbanes-Oxley Section 404 Compliance for iSeries White Paper*, July 21, 2004, page 3.

these accounts could go unnoticed for a long time." For our review, we identified DDS employees with inactive profiles and PINs unused[22] over 120 days and over 365 days, respectively.[23] Tables 1 and 2 summarize the results of our review.

Table 1: Inactive Profiles

Total Employees Reviewed	Total Employees with a Profile(s) Unused for more than 120 days	Total Employees with a Profile(s) Unused for more than 365 days
9,785	512	709

We noted for all 14 DDSs, 512 employees (5 percent of all employees) had at least 1 profile that was unused for over 120 days. For example, 1 State had 11 of 802 employees with profiles that were unused over 120 days, which totaled 1.4 percent. We also found 1 State had 35 of 216 total employees with unused profiles over 120 days, which totaled 16.2 percent.

We also noted about 7 percent, or 709 employees, had at least 1 profile that had not been used in over 365 days. For instance, we found that 5 States had over 10 percent of their employees with profiles unused for more than 365 days. One of these States had 40 of its 216 (18.5 percent) employees with at least 1 profile unused for over 365 days. Because of the length of time in which the profiles had not been used, it appears that they are not necessary for the employees to complete their job functions. The additional access increases the risk of claimant data being accessed inappropriately.

Table 2: Inactive PINs[24]

Total Employees Reviewed	Total Employees with PINs Unused for more than 120 days	Total Employees with PINs Unused for more than 365 days
9,785	135	139

PINs are assigned to each user to act as the user's "name" in the system. When a user signs into the system, the date of access is captured in Top Secret. Based on our review of user PINs that had been unused for a period of time, we noted that 135 (approximately 1 percent) of all DDS employees from all 14 DDSs had not signed into their accounts in more than 120 days, and an

[22] The number of days unused for the PINs indicates how many days it has been since the user last signed on.

[23] Because an individual can be assigned a positional and several functional profiles, an employee may be included in more than one of the results tables.

[24] One State did not have any employees with PINs unused over 120 days.

additional 139 (1 percent) had not signed onto their accounts in more than 365 days. For instance, we noted 1 State had 12 employees (5.6 percent) that had not signed onto their accounts in over 120 days and an additional 13 (6 percent) that had not accessed their accounts in over 365 days. DDSs need to ensure that inactive accounts are removed timely to reduce the risk of inappropriate access to claimant data. See Appendix C for a breakout of results for each State tested.

Terminated Employees

We obtained a list of terminated employees from each of the 14 DDSs through April 2011 to determine whether the employees' access had been deactivated[25] timely from the date of separation.[26] According to SSA policy, employees should be removed from the system immediately when they are terminated or separated from the DDS. Although SSA policy states that access should be removed immediately, we identified employees' accounts that were not deactivated within 5 business days of the date of separation provided by the DDS. Table 3 summarizes the results of our review.

Table 3: Number of Days to Deactivate PINs for Terminated Employees

Number of Days from Employee Separation to Deactivation of PIN	Number of States	Number of Employees
6 business days to 30 days	9	56
31 to 60 days	9	30
61 to 90 days	5	9
Over 90 days	13	91

During our review of terminated employees, we also noted (1) accounts that had an inactive status[27] and had not been deactivated by the Security Officer, (2) accounts that were still active, and (3) temporary employees that left the DDS for a period of time and returned to work; however, access was either never deactivated or deactivated untimely. We contacted the DDSs to confirm that each of these individuals had been removed from the DDS. We also obtained updated reports[28] to determine whether the employees' statuses had changed since the DDSs were notified of the results.

---

[25] An account is deactivated when a user's access on the system is suspended, rendering the account useless for the purpose of gaining further systems access.

[26] We tested 424 terminated employees.

[27] According to the Agency, an account becomes inactive after 59 days of nonuse unless a Security Officer makes the PIN inactive. If a PIN is inactive, a Security Officer has to reactivate it before it can be used to access the system.

[28] We obtained "History" reports from Top Secret to identify the status of the accounts and date on which the account was deactivated.

Accounts with Inactive Status

We noted 5 States that had a total of 12 employees with an inactive status. According to the report detail, there was no indication that these accounts had been deactivated. We provided the five DDSs with the employee names to confirm they were actually separated from the DDS. According to all five DDSs, all of the employees had separated from the DDSs. We obtained updated reports as of May and again in October 2012 to determine whether the status of these accounts had changed. Table 4 summarizes the results.

Table 4: Updated Status of Inactive Accounts as of May and October 2012

Updated Status of Inactive Accounts	As of May 2012		As of October 2012	
	Number of States	Number of Employees	Number of States[29]	Number of Employees
Accounts were deactivated but it was over 90 days since the date of separation	1	2	3	7
Accounts were still inactive and had not been deactivated by the Security Officer	4	10	3	5

Accounts with Active Status

We noted 9 States with 56 employees who still had active accounts despite the DDSs stating they had separated from the DDS. We provided the DDSs with the names of the employees to confirm that they had actually separated from the DDS. According to all nine DDSs, all but one individual had been separated from the DDSs. We obtained updated reports as of May and again in October 2012 to determine whether the status of these accounts had changed. Table 5 summarizes our results.

[29] One State had both employees that were deactivated and an employee that was still inactive.

Table 5: Updated Status of Active Accounts as of May and October 2012

Updated Status of Active Accounts	As of May 2012		As of October 2012	
	Number of States	Number of Employees	Number of States	Number of Employees
Accounts were deactivated but it was 31 to 60 days since the date of separation	1	1	1	1
Accounts were deactivated but it was 61 to 90 days since the date of separation	1	2	1	2
Accounts were deactivated but it was over 90 days since the date of separation	9	43	9	47
Accounts were still active and had not been deactivated by the Security Officer	4	9	1	5

For the employees who still had an active status, we also obtained a report from Top Secret showing specific detail of the PIN including the date it was last used.[30] We noted that for one employee, the date the PIN was last used was after the date of separation provided by the DDS. For this individual, the date of last use was in November 2010, and this employee left the DDS in August 2010. We provided this case to Headquarters for review on August 3, 2012. According to the Agency, systems staff used this PIN in troubleshooting workstation components and applications in the user group that allows login script customizations, rights/permissions, software usage and performance and compact disc creation. When a PIN is not deactivated upon separation and is allowed to be used by other staff, the Agency's data are at risk for individuals not approved to access SSA systems.

Temporary Employees

During our inquiries with the DDSs, we noted several employees whom the DDSs stated had separated but, upon further review, noted that they had returned to the DDS or transferred to another DDS after a period of separation. We found for three States, four employees had separated for a period of time or switched to another location; however, the PINs were not deactivated during the period of separation. For example, one State had an employee who left the DDS in September 2010. During our review of the Top Secret reports, we noted this individual still had an active account. Based on follow up with the DDS, we were informed that this employee returned in March 2011. According to the Top Secret report, this account was not deactivated when the employee separated. For another State, the DDS stated the individual left the DDS in March 2011. According to Top Secret, this account was not deactivated. Upon

[30] The last used field is populated by Top Secret whenever the user connects to the mainframe. It is updated upon a successful login.

further discussion with the DDS, we were informed that the employee was working at a different DDS, and Top Secret was not updated to show the new location.

We also noted one State had two employees who left temporarily; however, the DDS did deactivate the accounts when the employees left. We noted that one account was deactivated 20 days after the date of separation, and one account was deactivated 45 days after the employee left the DDS. DDSs need to ensure that all accounts are deactivated timely after an employee has separated. When separated employees' systems access is not removed timely, they may have inappropriate access to SSA systems.

Procedures for Deactivating and Deleting PINs

We noted that procedures the DDSs followed for deactivating PINs upon an employee's separation were not consistent among DDSs. For instance, we found that Security Officers at DDSs in 11 States were responsible for deactivating the employee's access. However, the remaining three DDSs stated the regional office's CSI was responsible for deactivating the accounts. SSA policy states that DDS Security Officers are responsible for certain PIN maintenance, such as discontinuing authorized systems access during an employee's departure. Although the policy says the DDS Security Officer should take action, it is not clear whether it is the Security Officer's responsibility to actually deactivate the accounts or notify the regional office CSI. Without a consistent policy in place for DDSs, accounts may not be deactivated timely and therefore are at higher risk of inappropriate access to claimant data.

We also noted that there was no consistent process for deleting PINs once an employee separated from the DDS. According to the Agency, each region follows a different process for requesting an account be deleted from Top Secret. There is no required form that DDSs complete to request the removal of access when an employee is terminated. Therefore, the accounts for employees who have been terminated are not timely removed from Top Secret, leaving their access vulnerable to inappropriate use. Policy does not seem to be clear on who has the authority over the process for deactivating and deleting accounts.

DDS Documented Process

To ensure the DDSs had appropriate processes in place for requesting and approving access to SSA's systems, we requested the formal internal documentation from each DDS outlining the process. Nine of the DDSs could not provide formal internal documentation. Some States said employees understood the process, and they received training on the process. Other States said they relied on what SSA had documented either in POMS or on regional sites. According to SSA policy, each DDS must have a procedure that documents its users' access. Although POMS is not specific about whether the DDSs should formally document this process, having undocumented policies and procedures for accessing SSA systems may result in an ineffective method of reviewing the request for such access. This could lead to users obtaining or retaining inappropriate authorization to SSA systems and information.

CONCLUSIONS

Controlling and limiting access to the Agency's information systems and resources is the first line of defense in ensuring the confidentiality, integrity, and availability of the Agency's information resources. Lack of adequate access controls compromises the completeness, accuracy, and validity of the information in the system.

Although the Agency has controls in place, such as the TEC, we found that DDS employees were granted unnecessary access. Specifically, we noted that DDS employees were assigned profiles that were not appropriate for their job functions. We also found employees had profiles that had not been used for an extended period of time. According to SSA policy, DDS management must ensure that all user accounts are reviewed periodically and inactive accounts are disabled. Additional access can lead to unauthorized entry to the system.

Upon an employee's separation, their access should be deactivated immediately. We noted DDS employees who were separated from the DDS, and their access was not deactivated timely. For instance, one DDS deactivated an employee's account 943 days after the employee had separated from the DDS. By not removing separated employees' system access timely, personnel may have inappropriate access to SSA systems. A consistent process among DDSs for deactivating access and requesting accounts to be deleted would help ensure access was removed timely. According to the Agency, each region followed a different process to request an account to be deleted. The Agency should ensure a process is in place for all DDSs for deactivating and deleting accounts.

We also found that DDSs did not have formally documented policies and procedures regarding employees obtaining access to SSA systems. Undocumented policies and procedures detailing the process to obtain access to SSA systems may result in an ineffective method to review requests for such access. It could also lead to users retaining inappropriate authorization to SSA systems and information.

The previous two issues were also identified during the Fiscal Year 2011 financial statement audit. As such, Grant Thornton, LLP made the following recommendations.

- DDS management should follow Agency established separation procedures and ensure the timely removal of logical access for separated employees, and

- DDS management should document formal policies and procedures detailing the process for obtaining local access to SSA systems.

RECOMMENDATIONS

The Agency responded that it would issue a security reminder for the timely removal of access for separated employees and investigate revising POMS for the documentation of policies and procedures. Because these issues were previously identified and still ongoing, the Agency should strengthen policy to ensure that systems access for DDS employees is monitored and maintained properly. Therefore, we recommend SSA:

1. Establish policy and guidelines that sets a threshold for profile nonuse and assigns responsibility for removing nonuse profiles to DDS management.

2. Establish monitoring tools to alert DDS management when nonuse profiles are in excess of thresholds to ensure that proper action is taken timely.

3. Establish a policy that assigns responsibility for deactivating and deleting DDS user accounts and provide enforcement to ensure that access for separated employees and inactive user accounts is removed or disabled timely.

4. Establish policy that assigns responsibility to DDS management to document and enforce access management procedures that comply with SSA's information security policy.

AGENCY COMMENTS

SSA agreed with the recommendations. See Appendix C for the Agency's Comments.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objectives, we:

- Reviewed applicable Federal laws and regulations as well as SSA's policies and procedures pertaining to DDS systems access.
- Requested and reviewed State policy for establishing and maintaining systems access from each of the 14 DDSs.
- Obtained employee lists and assigned profiles from the Office of Telecommunications and Systems Operations for the 14 State DDSs as of March 15, 2011.
- Requested job titles and descriptions for employee lists from each of the 14 State DDSs.
- Selected a random sample of 45 employees from each of the 14 State DDS employee listings to compare the job title and description with the assigned profiles.
- Obtained the eTrust Cleanup Report as of April 15, 2011 for all employees from each of the 14 State DDSs.
- Requested a list of terminated employees including the date of termination through April 2011 from each of the 14 State DDSs.
- Obtained History reports from the Top Secret system for each of the terminated employees from all 14 State DDSs.

We determined that the computerized data used during our review were sufficiently reliable given our objectives, and the intended use of the data should not lead to incorrect or unintentional conclusions.

We performed our fieldwork at Headquarters in Baltimore, Maryland, from September 2011 through September 2012. 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 the evidence obtained provides a reasonable basis for our findings and conclusion based on our audit objectives.

Appendix B – Inactive Profiles and PINs per State

State	Total number of Employees	Number of Employees with Profiles Unused over 120 days	Number of Employees with Profiles Unused over 365 days	Number of Employees with PINs Unused over 120 days	Number of Employees with PINs Unused over 365 days
1	86	5	11	0	2
2	401	23	61	3	1
3	1,150	28	61	10	15
4	451	39	51	12	15
5	279	7	5	4	1
6	802	11	9	2	1
7	701	23	63	4	12
8	1,392	70	52	29	17
9	767	50	137	11	11
10	432	9	37	3	5
11	1,113	27	47	2	6
12	216	35	40	12	13
13	215	18	16	6	1
14	1,780	167	119	37	39

Appendix C – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: January 7, 2013 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Dean S. Landis /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "Access to Social Security Administration Data at the Disability Determination Services" (A-15-11-01127)--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 Amy Thompson at (410) 966-0569.

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "Access to Social Security Administration Data at the Disability Determination Services" (A-15-11-01127)

Recommendation 1

Establish policy and guidelines that sets a threshold for profile nonuse and assigns responsibility for removing nonuse profiles to DDS management.

Response

We agree.

Recommendation 2

Establish monitoring tools to alert DDS management when nonuse profiles are in excess of thresholds to ensure that proper action is taken timely.

Response

We agree.

Recommendation 3

Establish a policy that assigns responsibility for deactivating and deleting DDS user accounts and provide enforcement to ensure that access for separated employees and inactive user accounts is removed or disabled timely.

Response

We agree.

Recommendation 4

Establish policy that assigns responsibility to DDS management to document and enforce access management procedures that comply with SSA's information security policy.

Response

We agree.

Appendix D – Major Contributors

Victoria Vetter, Director, Financial Audit Division

Judith Kammer, Audit Manager, Financial Audit Division

Kelly Stankus, Senior Auditor

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 (http://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 http://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at http://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:	http://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