OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S IMPLEMENTATION OF PROGRAM OPERATIONS MANUAL SYSTEM SECURITY REQUIREMENTS FOR DISABILITY DETERMINATION SERVICES

May 2009 A-14-08-18076

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.
- Promote economy, effectiveness, and efficiency within the agency.
- Prevent and detect fraud, waste, and abuse in agency programs and operations.
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.
- Access to all information necessary for the reviews.
- Authority to publish findings and recommendations based on the reviews.

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: May 27, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Follow-up: The Social Security Administration's Implementation of Program Operations Manual System Security Requirements for Disability Determination Services (A-14-08-18076)

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) implemented recommendations in the following Office of the Inspector General (OIG) reports and PricewaterhouseCoopers (PwC) Management Letters.

- *General Controls of the Alabama Disability Determination Services Claims Processing System Need Improvement* (A-14-02-22089)

- *General Controls of the Washington Division of Disability Determination Services Claims Processing System Need Improvement* (A-14-02-22093)

- PwC Management Letters issued for its Fiscal Years (FY) 2001 through 2007 financial statement audits

We limited our review to those recommendations that requested modifying the Program Operations Manual System (POMS) privacy and security procedures for disability determination services (DDS).

BACKGROUND

The Disability Insurance program provides benefits to wage earners and their families in the event the wage earner becomes disabled. The Supplemental Security Income program was designed to help aged, blind, and/or disabled people who have little or no income. SSA implements the policies governing the development of disability claims under each program. Disability determinations under both programs are performed by DDSs in each State or other responsible jurisdiction according to Federal regulations.[1]

[1] 20 C.F.R., part 404, subpart Q, and part 416, subpart J.

Each DDS determines claimants' disabilities and ensures there is adequate evidence to support its determinations. On behalf of SSA, DDS personnel process and store personally identifiable information (PII),[2] such as names and Social Security numbers.

POMS[3] contains required and recommended privacy and security policies for DDSs. Those that address maintaining and safeguarding SSA's systems of records are mandatory, while those that address DDS facilities and personnel are discretionary provided they do not conflict with State security directives. To ensure the information SSA entrusts to the DDSs is protected in accordance with Federal laws and regulations as well as Agency policies and procedures, it is critical for SSA to keep POMS current and complete and monitor the DDS' compliance with POMS.

SSA issued new DDS privacy and security policies in August 2001; therefore, we determined whether SSA incorporated recommended changes to POMS from that date. The OIG made recommendations in 2002 and 2003, and PwC, under the direction of the OIG, made recommendations during its 2001 through 2008 annual audits. In these audits, PwC tested general controls at three DDSs, issuing Management Letters with recommendations to improve DDS' general controls.

We determined the status of the recommendations made in these reports. For those recommendations implemented, we performed limited compliance testing. For those recommendations not implemented, we reviewed SSA's basis for non-implementation and re-assessed the need for implementation based on mitigating controls in POMS. For additional information on our scope and methodology, see Appendix B.

RESULTS OF REVIEW

SSA implemented most of the recommendations[4] in two OIG reports and seven PwC Management Letters that requested modifying the POMS privacy and security procedures for DDSs. The following table summarizes the number of recommendations implemented and unimplemented as well as the total number of recommendations addressed in this report.

[2] Office of Management and Budget (OMB) Memorandum M-07-16 defines PII as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[3] POMS, DI 39567, *DDS Privacy and Security.* Before October 1, 2005, the DDS privacy and security policies were contained both in POMS and the DDS Security Document (DSD). On that date, however, the DSD was incorporated into POMS.

[4] The OIG reports and PwC Management Letters presented 37 recommendations that recommended 44 changes to POMS. We considered each recommended change to POMS to be one recommendation.

Recommended Changes to POMS		
Implemented	Unimplemented	Total
32	12	44

Of the 32 implemented recommendations, we performed limited compliance testing on the 28 implemented before October 2008.[5] Although new POMS requirements were released in October 2008, we did not test the compliance of the four recommendations addressed in that release to allow the DDSs time to make any necessary changes. Most noncompliance found during testing related to DDS security plans or was minor and related to inadequate documentation of procedures.

For the 12 unimplemented recommendations, we reviewed SSA's basis for rejection and mitigating controls in POMS to determine which recommendations we believe the Agency still needs to implement. We found that SSA had compensating controls in place for 11 of the unimplemented recommendations, and we consider these recommendations addressed. However, the Agency should reconsider and implement the remaining recommendation, which related to parking garage access controls.

Implemented Recommendations

SSA implemented 32 recommendations to revise POMS. These recommendations addressed the following security topics.

- Physical security requirements at the perimeter and sensitive areas in DDS facilities.
- Separation procedures for terminated personnel and removing sensitive equipment/information.
- Criminal background checks for new hires.
- Limited system access and guidance on reviewing security violation reports.
- The sufficiency, format and management review of the DDS security plan, including expanding contingency plan procedures to ensure continuity of operations at DDS facilities.

In response to the recommendations to improve DDS security policy, SSA updated the DSD and relevant POMS chapters numerous times between December 2001 and October 2008. While establishing policy is important, compliance with policy is equally important. As a result, we performed limited compliance testing on the 28 recommendations implemented before October 2008. Most noncompliance issues were related to DDS security plans or inadequate documentation of procedures.

[5] The remaining four recommendations were implemented in October 2008. Since these recommendations were recently added to POMS, we have not tested them in the DDSs. See Appendix C for details on the recommendations.

Among the implemented recommendations tested were specific requirements for security plan content and the plans' annual review by DDS management. Despite these requirements, two of three DDS security plans reviewed in 2008 did not comply with POMS. Furthermore, in 2006 and 2007, two of three plans reviewed were missing at least half the prescribed sections. We, therefore, recommend POMS require that Regional Office staff annually review the security plans and submit approvals or modification requests to the DDSs.

SSA implemented four recommendations in the October 2008 release of POMS, two of which were added after we brought the issues to the Agency's attention. Although the new POMS requirements were effective in October 2008, we did not test the compliance of the four recommendations implemented in that release because the DDSs did not have adequate time to make any necessary changes.

Unimplemented Recommendations

SSA considered, but did not implement, 12 of 44 recommendations.[6] Eleven of these recommendations have been mitigated through compensating controls;[7] however, the following recommendation has not been mitigated and needs to be incorporated into POMS.

- SSA should issue guidance for DDS security management to document and follow formal procedures for checking vehicles prior to allowing them entrance into the DDS parking garage. The door to the parking garage should remain closed until the person or vehicle attempting to enter the garage is verified by the guards.

We recognize current arrangements may not permit DDSs to control parking garage access; however, POMS must address this issue to ensure DDSs consider this action in the future.

CONCLUSION AND RECOMMENDATIONS

We found SSA implemented the majority of the recommendations made in two OIG reports and seven PwC Management Letters that requested modifying POMS privacy and security procedures for DDSs. However, to further improve the security program administered by all DDSs, we recommend that SSA modify POMS to:

1. Require that Regional Office staff annually review DDS security plans and submit approvals or modification requests to the DDSs.

[6] See Appendix C for a full list of recommendations.

[7] See Appendix D for a list of the 11 recommendations and mitigating controls.

2. Implement the prior recommendation to provide guidance for DDS security management to document and follow formal procedures for checking vehicles prior to allowing them entrance into the DDS parking garage. The door to the parking garage should remain closed until the person or vehicle attempting to enter the garage is verified by the guards.

AGENCY COMMENTS

SSA agreed with our recommendations. The Agency's comments are included in Appendix E.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

CDP	Center for Disability Programs
C.F.R	Code of Federal Regulations
CSI	Center for Security and Integrity Programs
DDS	Disability Determination Services
DSD	Disability Determination Services Security Document
FY	Fiscal Year
IDS	Intrusion Detection System
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	Personal Identification Number
POMS	Program Operations Manual System
PwC	PricewaterhouseCoopers
SSA	Social Security Administration

Scope and Methodology

The objective of this follow-up review was to determine whether the Social Security Administration (SSA) implemented recommendations in two Office of the Inspector General (OIG) reports and seven PricewaterhouseCoopers (PwC) Management Letters issued for its Fiscal Years 2001 through 2007 financial statement audits.

Our scope was limited to those recommendations that requested changes to the Program Operations Manual System (POMS) privacy and security procedures for the disability determination services (DDS). Thirty-seven recommendations fell within this scope, recommending 44 changes to POMS.

To accomplish our objective, we:

- Extracted all recommended changes to the POMS privacy and security procedures the DDSs should follow. Each recommended change was treated as a single recommendation.
- Traced each implemented recommendation to the language that was used to implement it in POMS.
- Reviewed those recommendations unimplemented by the Agency to determine which should be reconsidered for incorporation into POMS.

To assess the implementation of recommendations at the DDSs, we also performed a limited compliance review on the 28 recommendations that were incorporated into POMS before October 2008. Although new POMS requirements were released in October 2008, we did not test the compliance of the four recommendations implemented in that release since the DDSs had not had adequate time to make the necessary changes.

To perform our testing, we partially relied on the work done by PwC during its financial statement review. During its FY 2008 audit, PwC tested 16 recommendations at 3 DDSs. An additional two recommendations concerned triennial reviews, which were last tested during PwC’s FY 2006 audit. Most noncompliance found during testing related to DDS security plans or was minor and related to inadequate documentation of procedures.

To provide a sufficient basis to rely on the work done by PwC staff, we:

- Obtained and reviewed evidence concerning the staff's qualifications and independence.
- Obtained and reviewed the latest peer review report on PwC to determine whether the firm had an adequate quality control process in place as of June 2006.
- Reviewed the scope and quality of the work performed at the DDSs and the supporting documentation for its Management Letter findings.
- Reviewed the audit program steps followed for the DDS security tests.

For the remaining 10 recommendations, we conducted limited compliance tests in 5 of the 10 SSA regions. In each of those five regions, we had SSA determine which DDSs had excessed computers. We chose five DDS sites (Maryland, Kansas, New York, Massachusetts and Louisiana) for review. We used computer forensics software to determine whether excessed computer hard drives at these sites had been properly erased per POMS. We also determined whether these five DDSs were complying with the other nine recommended changes to POMS implemented before October 2008 not tested by PwC. We noted one instance of noncompliance; however, because of compensating controls, it did not rise to the level of an exception.

We performed our field work at SSA Headquarters between November 2007 and December 2008. The entity audited was the Office of Operations. 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Status of Reviewed Recommendations

The table below identifies whether the Social Security Administration (SSA) implemented recommended changes to the Program Operations Manual System made in two Office of the Inspector General (OIG) reports and seven PricewaterhouseCoopers (PwC) Management Letters issued for its Fiscal Years 2001 through 2007 financial statement audits. These reports recommended 44 changes to POMS. Of these recommended changes, 32 were implemented and 12 were not implemented.

Recommendation	Source	Category	Part	Implemented
1a	PwC 2003	Physical Security	Include requirements in the DDS Security Document to use access mechanisms that are not based on cipher locks, the code for which is easily disclosed.	No
1b	PwC 2003	Physical Security	Use access mechanisms that can log entrances and exits to provide proper audit trails.	
2a	Washington	Physical Security	Clarify that perimeter security guidelines extend to elevators accessing DDS operations when the DDS is in a multi-tenant building.	No
2b	Washington	Physical Security	Add requirements on the control and security of elevators used to access secure DDS operations.	
2c	PwC 2003	Physical Security	Install locking doors with card readers outside the elevators on each of the DDS floors.	
3a	Alabama	Physical Security	Expand the building perimeter security guidance to include the security of lobby entrances into DDS operational areas.	Yes
3b	Washington	Physical Security	Clarify that perimeter security guidelines extend to DDS entrances in addition to building entrances when the DDS is in a multi-tenant building.	
4	PwC 2006	Physical Security	Update the DDS annual self review checklist to require DDS management to perform an annual recertification of personnel with physical access to the DDS, including sensitive areas of the DDS, such as the computer room.	Yes (10/08)
5a	Alabama	Physical Security	Require the installation of burglar alarm system devices in computer and telephone rooms if a perimeter burglar alarm system has not been installed .	No

Recommendation	Source	Category	Part	Implemented
5b	PwC 2003	Physical Security	The DDS computer room should be secured with alarms, motion sensors or other detection devices to identify unauthorized access during times when the computer room staff is not present. Such devices should automatically notify a monitoring center.	
6	Alabama	Physical Security	Guidance and instruction to provide a consistent framework (types, use and placement) for burglar alarm system devices and smoke detectors in a DDS.	No
7	PwC 2003	Physical Security	Install automatically closing computer room doors.	Yes (10/08)
8	Alabama	Physical Security	Clearly state that computer room locks should be keyed separately from the building master keys.	Yes
9	Alabama	Physical Security	Guidance on the control and security of a telephone room when the telephone system is located in a separate room from the computer room.	Yes
10	PwC 2002	Physical Security	Update the DDS Security Document to include specific guidance related to the protection of the computer rooms that do not have true walls that extend from floor to ceiling. This guidance should include alternate methods to secure the computer rooms other than extending the walls. A common practice is to install chain link fences, heavy wire mesh, or motion sensor alarms in the space between the false ceiling and the true ceiling of the facility.	Yes
11	Alabama	Physical Security	Guidance and security procedures for computer rooms located on a perimeter wall with windows.	Yes
12	PwC 2003	Physical Security	Completely enclose the wiring closets.	Yes
13a	PwC 2003	Physical Security	The door to the parking garage should remain closed until the person or vehicle attempting to enter the garage is verified by the guards.	No
13b	PwC 2003	Physical Security	DDS security management should formally document (and ensure the guards are consistently following) formal procedures for checking vehicles prior to allowing them entrance into the DDS parking garage.	

Recommendation	Source	Category	Part	Implemented
14	PwC 2007	Physical Security	Update the POMS guidelines to specifically include the authentication of visitors to a government issued photo ID (driver's license, passport, state-issued ID badge) prior to entering the DDS facility.	Yes
15	PwC 2004	Physical Security	Complete a risk assessment to determine if metal detectors or X-ray machines would be an appropriate solution for this weakness.	No
16a	PwC 2003	Physical Security	Address the physical security concerns by screening personnel and packages at the entrances to the DDS facility. The requirement to perform this procedure should be added to the DDS Security Document.	Yes (10/08)
16b	PwC 2004	Physical Security	Develop procedures to inspect the belongings of personnel and visitors entering the facility.	
17	Alabama	Physical Security	Guidance on conducting a risk-based, cost-benefit analysis to determine whether existing and future DDS buildings without a sprinkler system should have one installed.	No
18	PwC 2002	Access Control	Provide DDS management with detailed guidance and procedures that should be completed when the DDS is disposing of or removing sensitive information or equipment from the DDS.	Yes
19	PwC 2002	Access Control	Update the DDS Security Document to ensure that specific guidance is given with relation to the separation procedures for terminated (or extended leave) or separated employees. This guidance should include all activities that are required to take place during employee exit procedures, including the return of property and the removal of access amounts from system and application environments.	Yes
20	Washington	Access Control	Add requirements to change shared entrance combinations whenever DDS personnel cease employment.	Yes
21a	PwC 2002	Suitability	Require all DDS employees to complete an employee suitability review process. These reviews should be conducted in a manner that is consistent with the overall SSA policies related to employee background checks.	Yes (10/08)

Recommendation	Source	Category	Part	Implemented
21b	PwC 2002	Suitability	Basic background checks performed for all employees of the DDS to ensure a reduction in the risk of hiring personnel that have past criminal records. The background checks should be performed in a consistent manner with overall SSA background investigation procedures.	
22	Alabama	Suitability	Guidance that requires conformity with SSA's suitability program.	No
23a	Alabama	Technical Security	Guidance to specify security training requirements for DDS security officers to obtain and maintain their skills in administering security on an AS/400 or other DDS system.	No
23b	Washington	Technical Security	Establish security officer training requirements that comply with Federal standards.	
24	Alabama	Technical Security	Guidance to specify the duties DDS security officers should not perform.	No
25	Alabama	Technical Security	Guidance on access control procedures relating to approving and documenting DDS system initial requests, access changes and terminations.	Yes
26	Alabama	Technical Security	Guidance to restrict access and limit the use of communication ports in DDS systems.	Yes
27	Alabama	Technical Security	Guidance on access control procedures relating to using naming standards for profiles and group and temporary profiles.	No
28	Alabama	Technical Security	Guidance to restrict access and limit the use of generic profiles including vendor supplied profiles.	Yes
29	Alabama	Technical Security	Guidance to restrict access and limit the use of security-related operating system commands.	Yes
30	PwC 2006	Technical Security	Update POMS to specify the timeframe in which security violation reports should be reviewed by DDS management.	Yes
31	Alabama	Technical Security	Guidance on access control procedures relating to monitoring, reviewing, and reporting DDS system security violations.	Yes
32a	PwC 2002	Security Plan	Update the DDS Security Document to ensure that specific guidance is given related to the completion of annual security and sanction awareness activities for all DDS employees.	Yes

Recommendation	Source	Category	Part	Implemented
32b	PwC 2002	Security Plan	Provide guidance to ensure the employees are reviewing and signing the awareness documentation on an annual basis.	
33	PwC 2002	Security Plan	Identify a specific list of possible DDS or field office sites for each DDS and coordinate agreements related to the accommodation of additional workload.	Yes
34	PwC 2002	Security Plan	Identify needs in a worst-case scenario.	Yes
35	PwC 2003	Security Plan	Document policies and procedures regarding actions to be taken for each of the Department of Homeland Security threat levels.	No
36	PwC 2002	Security Plan	Establish and document a clear definition of what work will be performed at the alternate sites.	Yes
37	Alabama	Security Plan	Detailed back-up procedures for copies of the contingency plan.	Yes
38	Washington	Security Plan	Create a formal risk-based security control review that is used at least every 3 years or whenever a major system modification occurs.	Yes
39a	Alabama	Security Plan	Detailed back-up procedures for the storage of back-up files.	Yes
39b	PwC 2004	Security Plan	Update the DDS Security Document to define a standard rotation schedule to maintain back-up tapes at an off-site storage facility for specified amount of time.	
40a	PwC 2002	Security Plan	Ensure that the DDS security guidance is updated to require management reviews of DDS security plans. This guidance should be in line with the overall SSA policies for security plan currency.	Yes
40b	PwC 2002	Security Plan	Ensure that evidence be maintained of these reviews. This guidance should be in line with the overall SSA policies for security plan currency.	
41a	Alabama	Security Plan	DDS continuity of operations plan requirements recommended by PwC in its *FY 2001 Management Letter*.	Yes
41b	Alabama	Security Plan	DDS security plan contents that comply with OMB Circular A-130, Appendix III requirements, as recommended by PwC in its *FY 2001 Management Letter*.	

Recommendation	Source	Category	Part	Implemented
41c	PwC 2002	Security Plan	Ensure that POMS 39566.120 is updated to include all requirements of OMB A-130 Appendix III with regard to security requirements. This will ensure that the DDS plans are updated in a correct format.	
42	Washington	Security Plan	Require the management of each DDS to certify at least every 3 years that the security controls are sufficient to warrant the continued use of each DDS general support system and major application.	Yes
43a	Alabama	Security Plan	Guidance on access control procedures relating to conducting annual reviews of all access privileges on DDS and SSA systems.	Yes
43b	PwC 2002	Security Plan	A periodic review should be performed for the mainframe, NT, WANG, and AS400 (when fully implemented) to ensure that users have only been granted access necessary to fulfill job responsibilities.	
43c	PwC 2002	Security Plan	Annual reviews of NT, AS 400, and mainframe access required by the DDS Security Document.	
43d	PwC 2002	Security Plan	Access to the mainframe compared by using the actual access listings from Top Secret to compare to job requirements.	
44a	PwC 2002	Security Plan	Ensure that the DDS Security Document is updated to include specific guidance related to the policies for completing annual recertification of personnel with access to the WANG, NT, and AS400 environments.	Yes
44b	PwC 2002	Security Plan	SSA policy modified to require documentation of access reviews performed to match access to that granted by the Top Secret software.	

Appendix D

Mitigating Controls for Unimplemented Recommendations

The table below identifies 11 recommendations to modify the Program Operations Manual System (POMS) privacy and security procedures for disability determination services (DDS) that were not implemented by the Social Security Administration (SSA).[1] Although not implemented, we believe POMS contains mitigating controls that address the concerns of these recommendations.

Recommendation	Part	Mitigating POMS Control and Reference
1a	Include requirements in the DDS Security Document to use access mechanisms that are not based on cipher locks, the code for which is easily disclosed.	Change access codes, such as the intrusion detection system (IDS) code, combination/cipher lock codes, card access codes, and safe combinations when staff with knowledge of them leave or no longer have a need to know them, or whenever compromise of the codes occurs or is suspected. (DI 39567.040) Screen personnel, visitors, and packages at the entrance to the DDS facility. (DI 39567.025) If used by personnel, perimeter doors should have a combination/cipher lock or a card access system. (DI 39567.015)
1b	Use access mechanisms that can log entrances and exits to provide proper audit trails.	
2a	Clarify that perimeter security guidelines extend to elevators accessing DDS operations when the DDS is in a multi-tenant building.	If a DDS is located in a multi-tenant building, it should be self-contained to the extent possible. (DI 39567.015)
2b	Add requirements on the control and security of elevators used to access secure DDS operations.	
2c	Install locking doors with card readers outside the elevators on each of the DDS floors.	

[1] See Appendix C for a full list of recommendations.

Recommendation	Part	Mitigating POMS Control and Reference
5a	Require the installation of burglar alarm system devices in computer and telephone rooms if a perimeter burglar alarm system has not been installed.	Install an intrusion detection system (IDS) in all facilities unless determined unnecessary. (DI 39567.020) Restrict computer room access to management or authorized personnel. (DI 39567.020)
5b	The DDS computer room should be secured with alarms, motion sensors or other detection devices to identify unauthorized access during times when the computer room staff is not present. Such devices should automatically notify a monitoring center.	
6	Guidance and instruction to provide a consistent framework (types, use and placement) for burglar alarm system devices and smoke detectors in a DDS.	Install an IDS in all facilities unless determined unnecessary. (DI 39567.020) Abide by local fire codes. (DI 39567.030)
15	Management should also complete a risk assessment to determine if metal detectors or X-ray machines would be an appropriate solution for this weakness.	Screen personnel, visitors, and packages at the entrance to the DDS facility. (DI 39567.025)
17	Guidance on conducting a risk-based, cost-benefit analysis to determine whether existing and future DDS buildings without a sprinkler system should have one installed.	Abide by local fire codes (DI 39567.030) Install an IDS in all facilities unless determined unnecessary (DI 39567.020)
22	Guidance that requires conformity with SSA's suitability program.	Although Federal regulations reserve governance of personnel matters to the States, we expect that each DDS will maintain and administer an effective suitability program. DI 39567.260 C in this section establishes the minimum requirement that DDS suitability programs include a statewide criminal background check. Beyond that minimum requirement, States are given broad discretion on the composition, implementation, and administration of their DDS suitability programs. (DI 39567.260)
23	Guidance to specify security training requirements for DDS security officers to obtain and maintain their skills in administering security on an AS/400 or other DDS system. Establish security officer training requirements that comply with Federal standards.	The DDS Security Officer is responsible for implementing SSA security policies and procedures so access to SSA data is properly controlled. In carrying out this responsibility, the DDS Security Officer must have the ability and maintain the systems skills to effectively monitor current systems in areas of certification and violation procedures. (DI 39567.320)

Recommendation	Part	Mitigating POMS Control and Reference
24	Guidance to specify the duties DDS security officers should not perform.	All users requiring access to SSA/DDS systems must submit Form SSA-120 to their DDS Security Officer to obtain a 6-digit personal identification number (PIN). (DI 39567.060) The DDS Security Officer reviews the form for accuracy and to ensure the user is assigned proper systems access to perform his or her work assignments. Part of the DDS Security Officer's review is to determine whether the user has already been assigned a PIN. If so, then the Security Officer provides the previously assigned PIN to the user after contacting the Center for Security and Integrity (CSI)/Center for Disability Programs (CDP) to reactivate it. If a new PIN is required, then the Security Officer signs the form as the requesting official, and forwards the form to the CSI/CDP. CSI reviews the form. If the employee requires access, then CSI approves the form and issues a PIN, or returns copies of the form to the DDS Security Officer with a previously assigned PIN. CSI or CDP retains the original and informs the DDS Security Officer of the new PIN. (DI 39567.060)
27	Guidance on access control procedures relating to using naming standards for profiles and group and temporary profiles.	All user profiles, including any generic profiles and profiles for non-DDS employees, should be supported by a DDS access procedure. This procedure should support the access privileges on the iSeries or other case processing system as well as what menu is provided for all DDS users in the State claims processing system. (DI 39567.080) Users who do not require a high level of access should have their status updated and special access removed. This review should be conducted on a periodic basis and must be performed at least annually. (DI 39567.105)
35	Document policies and procedures regarding actions to be taken for each of the Department of Homeland Security threat levels.	Each DDS must create and maintain a Continuity of Operations Plan as part of its DDS Security Plan. The local DDS information provided in the plan is supplementary to the Regional Office plan and is used to assist the Regional Office if continuity of operations efforts for the DDS should become necessary. (DI 39567.190)

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: May 08, 2009 Refer To: S1J-3

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

From: James A. Winn /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Follow-up: The Social Security Administration's Implementation of Program Operations Manual System Requirements for Disability Determination Services" (A-14-08-18076)—INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate the comprehensive work that the OIG auditing team did on this report. Our response to the report findings and recommendations is attached.

Please let me know if we can be of further assistance. Please direct staff inquiries to Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S IMPLEMENTATION OF PROGRAM OPERATIONS MANUAL SYSTEM SECURITY REQUIREMENTS FOR DISABILITY DETERMINATIONS SERVICES" (A-14-08-18076)

Recommendation 1

Require that regional office staff annually review disability determination services (DDS) security plans and submit approvals or modification requests to the DDSs.

Comment

We agree. We will consider updating Program Operations Manual System (POMS) DI 39567.160 to include a requirement that regional office staff review DDS security plans annually and provide approval or recommended modifications to each DDS.

Recommendation 2

Implement the prior recommendation to provide guidance for DDS security management to document and follow formal procedures for checking vehicles prior to allowing them entrance into the DDS parking garage. The door to the parking garage should remain closed until the guards have verified vehicle and/or person attempting to enter the garage.

Comment

We agree. We will update POMS DI 39567.015 with language recommending that DDSs with garage parking establish and follow formal procedures for checking vehicles prior to garage entry.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Phil Rogofsky, Acting Director, Information Technology Audit Division

Mary Ellen Moyer, Acting Audit Manager

Acknowledgments

In addition to those named above:

Alan Lang, Senior Auditor

Michael Zimmerman, Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-08-18076.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations,
House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.