OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

COMPLIANCE WITH
DISABILITY DETERMINATION SERVICES
SECURITY REVIEW REQUIREMENTS

February 2008 **A-05-07-17082**

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: February 6, 2008 Refer To:

To: The Commissioner

From: Inspector General

Subject: Compliance with Disability Determination Services Security Review Requirements (A-05-07-17082)

OBJECTIVE

Our objectives were to assess (1) the Social Security Administration's (SSA) procedures for selecting Disability Determination Services (DDS) offices for on-site Security Reviews, (2) SSA's system for ensuring appropriate correction of deficiencies identified through Security Reviews, and (3) additional steps SSA can take to enhance the Security Review process.

BACKGROUND

SSA must comply with applicable Federal law[1] associated with management controls and provide assurances that its financial, program and administrative processes are functioning as intended. SSA designed the Management Control Review (MCR) Program to satisfy such Federal requirements. The MCR Program is implemented at DDS offices using the DDS *Security Self-Review Checklist*. These reviews cover a number of systematic and physical security elements including (1) automated system security, (2) systems access, (3) perimeter and internal office security, and (4) emergency preparedness and disaster recovery.

There are 52 DDSs located in the 50 States, the District of Columbia and Puerto Rico. Each DDS is required to have a Security Review conducted by the Center for Security and Integrity (CSI) at least once every 5 years.[2] The CSI in each region is required to develop and maintain a 5-year review plan for all DDSs in its respective region. The plan should include all DDS locations to be reviewed.

[1] *Federal Managers' Financial Integrity Act of 1982*, Public Law 97-255.

[2] SSA, Program Operations Manual System (POMS), DI 39566.140 B.2.b., *DDS Compliance and Monitoring Procedures*.

Most of the Security Reviews are conducted by CSI; however, SSA also uses contractors to conduct Security Reviews on its behalf. In years when CSI does not conduct a Security Review, the DDS offices are responsible for conducting a self-review using the same criteria CSI uses for its Security Review.[3]

When performing the Security Review, CSI follows SSA policy in POMS,[4] which contains the DDS *Security Self-Review Checklist*.[5] Within 45 days of completing the Security Review, CSI prepares a report that describes the deficiencies identified during the review and provides recommendations to resolve the deficiencies. The report is submitted to the regional Center for Disability Programs (CDP) with copies to the Office of Disability Determinations and the Division of Financial Integrity. CDP provides the Security Review report to the DDS office.

RESULTS OF REVIEW

Generally, we found SSA's procedures were effective for selecting DDS offices for on-site Security Reviews and ensuring correction of deficiencies identified through Security Reviews. However, we found some improvements were needed. Specifically:

- we identified 6 DDS offices did not undergo a Security Review during the 5-year period ended September 30, 2006;

- 6 of 32 DDS offices undergoing a Security Review during the 2-year period ended September 30, 2006 did not submit a corrective action plan (CAP) in accordance with SSA requirements; and

- 29 of 122 Security Review deficiencies at 5 of the 9 DDS offices we reviewed were not corrected at the time of our review.

We also identified some areas that should be included in the Security Review process. Specifically, the DDS *Security Self-Review Checklist* could be more comprehensive, covering additional topics such as protection of sensitive data as well as properly securing computers and computer room doors.

---

[3] SSA, POMS DI 39566.140 B.1.b., *DDS Compliance and Monitoring Procedures*.

[4] SSA, POMS DI 39566, *DDS Privacy and Security*.

[5] SSA, POMS DI 39566.186, *Security Self-Review Checklist – Exhibit 7.*

DISABILITY DETERMINATION SERVICES OFFICES NOT REVIEWED

During the 5-year period ended September 30, 2006, we found that a Security Review was not conducted at six DDS offices in five regions. In Table 1, we identify the locations and the reasons Security Reviews were not conducted.

Table 1: Security Reviews Not Conducted

Region	Office Location	Status
I	Waterbury, Vermont	CSI postponed the Security Review until 2007 because the DDS office was undergoing electronic claims training in 2006.
II	Endicott, New York[1]	CSI considered a review conducted in 2004 by an independent contractor to be sufficient to meet the Security Review requirement.[2]
V	St. Paul, Minnesota	A Security Review was not conducted because regional policies prohibit travel to perform the reviews unless other work is to be conducted at the same location. Since no other work was scheduled at this location in Fiscal Year (FY) 2006, the year the Security Review was originally scheduled, the review was postponed until FY 2007.
VIII	Aurora, Colorado	CSI considered a review conducted in 2003 by an independent contractor to be sufficient to meet the Security Review requirement.[2]
IX	Tucson, Arizona[3]	A Security Review was not conducted because regional policies prohibit travel to perform the reviews unless other work is to be conducted at the same location. Since no other work was scheduled at this location in FY 2006, the year the Security Review was originally scheduled, the review was postponed until FY 2007.
	Sacramento, California (Central Operations)[4]	CSI established a 5-year review cycle that excluded the Sacramento, California DDS location from review. CSI plans to conduct the Security Review in 2007.

Note 1: The New York DDS is decentralized with offices in six locations.
Note 2: While the contractors in question reviewed security controls at selected DDS offices as a part of the annual Financial Statement audit, they were not engaged in this instance to conduct Security Reviews nor did they use the checklist that CSI uses for Security Reviews. Therefore, these reviews are not as comprehensive and cannot be considered as replacements for CSI Security Reviews.
Note 3: The Arizona DDS is decentralized with offices in two locations.
Note 4: The California DDS is decentralized with offices in 14 locations.

For the six DDSs that did not conduct Security Reviews, we reviewed our prior DDS administrative cost audits that assessed limited areas of the general security controls environment. In these reports, we noted general security control vulnerabilities in such areas as inventory controls, contingency plans, off-site storage for electronic backup files, intrusion detection systems, perimeter access, and controls over computer

security. For example, at the Minnesota DDS,[6] we found issues related to the need to

- finalize a contingency plan;
- identify an off-site storage facility for electronic data backup files; and
- review perimeter security.

Had our audit of the Minnesota DDS office not been performed, these previously identified security-related deficiencies could have gone undetected and even resulted in the loss or compromise of sensitive data. For this reason, we believe CSI should ensure all DDS offices are reviewed every 5 years or provide written justification if Security Reviews will not be performed.

CORRECTIVE ACTION PLAN

We found that 6 of 32 DDS offices (19 percent) undergoing a Security Review during the 2-year period ended September 30, 2006 did not submit a CAP in accordance with SSA requirements. Five of the DDS offices were late in submitting their CAPs, and the remaining DDS office has yet to submit a CAP.

The DDS is responsible for developing a CAP to address the deficiencies identified in the Security Review report. The CAP should be submitted to CDP within 45 days of the Security Review report's issuance date. CDP provides the CAP to CSI. Both CDP and CSI monitor the corrective actions until all weakness are corrected.[7] If a CAP is not submitted as required, there is a risk that deficiencies identified during Security Reviews will not be corrected, thereby allowing unauthorized access to sensitive SSA information. For this reason, SSA should instruct CDPs and CSIs to obtain CAPs that address all deficiencies identified during Security Reviews within the 45-day timeframe from all DDS offices.

Late Corrective Action Plans

We reviewed 32 DDS Security Review reports that were conducted in FYs 2005 and 2006, and found that CSIs issued all the reports within 45 days of the Security Review or soon thereafter. We also found most of the DDS offices submitted a CAP to address the Security Review deficiencies within 45 days of the Security Review report's issuance date. However, we found that five DDS offices in three regions did not submit a CAP to the regional CDP within 45 days of the Security Review, as shown in Table 2.

---

[6] SSA Office of the Inspector General, *Administrative Costs Claimed by the Minnesota Disability Determination Services* (A-05-04-14036), page 3, September 2004.

[7] SSA, POMS, DI 39566.140 B.2.f., *DDS Compliance and Monitoring Procedures*.

Table 2: DDS Offices That Did Not Submit Timely CAPs

Region	Office Location	Security Review Report Date	Date of Corrective Action Plan	Days Late
I	Concord, New Hampshire	3/29/06	6/21/06	39
III	Washington, District of Columbia	6/20/06	3/01/07	209
IX	Sacramento, California	2/24/06	5/18/06	38
	Roseville, California	2/24/06	5/10/06	30
	Carson City, Nevada	5/04/05	7/18/05	30

In Region III, we found the CDP did not effectively monitor receipt of the CAP from the District of Columbia DDS. While the Security Review was conducted in May 2006, the CAP was not submitted to CDP until March 2007. When asked about the delay, CDP staff stated this occurred because the DDS Director's attention was focused on the conversion to the electronic claims process and a construction project at the DDS. While we understand CAPs can be delayed because of competing priorities, 209 days is an unreasonable delay. The new Disability Program Administrator in the Region III CDP, assigned to monitor the District of Columbia DDS in January 2007, was not aware the CAP had not been submitted for the 2006 Security Review. When we inquired about the CAP, the DDS was contacted and the CAP was provided.

Missing Corrective Action Plan

In our review of the 32 DDS Security Reviews, we found that the Ohio DDS did not submit a CAP to the Region V CDP following its Security Review. As noted earlier, the DDS is responsible for developing a CAP to address the deficiencies identified in the Security Review. In addition to not obtaining a CAP for the Ohio DDS, we found the Region V CSI only required that the DDSs in its region take corrective action for sensitive data access deficiencies.[8] SSA policy states that its standards for protecting the DDS facilities are discretionary.[9] Furthermore, the deficiencies identified during DDS Security Reviews addressed physical security, and the Region V CSI considered recommendations that address physical security deficiencies as suggestions that do not require corrective action.[10] Therefore, the CSI left it to the Ohio DDS' discretion to determine whether corrective action should be taken on physical security deficiencies. We believe SSA should consider revising its discretionary standards for protecting DDS facilities so that CAPs address all deficiencies identified during Security Reviews, even if the DDS position is that it will take no corrective action.

[8] Region V CSI staff stated that they only expected responses from the DDS offices for deficiencies regarding systems issues or inappropriate profile assignments.

[9] SSA, POMS, DI 39566.010 A., *Disability Determination Services Physical Security*.

[10] Although not required by Region V CSI, the Indiana and Michigan DDSs did submit CAPs to Region V CDP on their own initiative.

SSA policy also instructs DDSs that are unable to meet a guideline for physical security to prepare a risk assessment plan to determine whether some or all of the discretionary measures should be included in their security program.[11] In its Security Review of the Ohio DDS office, the Region V CSI recommended corrective actions to address deficiencies found with (1) open shredder bins that contained sensitive information, such as earnings, dates of birth and social security numbers; (2) cases left on desks and cabinets overnight; and (3) after-hours cleaning. The Security Review report also reflects that CSI reminded the Ohio DDS to prepare a risk assessment. Additionally, the Region V CSI informed us that it had plans to request the DDSs in the region to perform a risk assessment on physical security deficiencies.

DEFICIENCIES NOT CORRECTED

We found 29 of 122 deficiencies (24 percent) at 5 of the 9 DDSs we reviewed had not been corrected as of February 2007.[12] Specifically, 20 of the unresolved deficiencies were identified in FY 2005, and 9 were identified in FY 2006. The deficiencies were in the areas of systems access, perimeter and internal office security, incident reporting, and emergency preparedness and recovery.

The DDSs initiated corrective action for nine deficiencies identified during the Security Reviews. However, the completion of corrective actions was delayed for six of the nine deficiencies because the DDSs were located in facilities that were controlled by State or private property managers (see Table 3). Therefore, the DDSs were required to obtain approval to make modifications necessary to correct the deficiencies identified during the Security Reviews. In addition, completion was delayed for three deficiencies because the DDSs had to seek guidance from SSA.

Table 3: Corrective Actions Initiated but Delayed

Region	Location	Date Security Review Performed	Delayed Actions Due to DDS in a State/Private Facility	Delayed Actions While DDS Awaits Guidance from SSA	Total Delayed Actions
III	Roanoke, Virginia	February 2005	1		1
VI	Albuquerque, New Mexico	March 2005	1	1	2
		March 2006	2	2	4
IX	Carson City, Nevada	May 2005	2		2
Total			**6**	**3**	**9**

For the remaining 20 deficiencies identified during the Security Reviews, the DDSs indicated that corrective action was not planned. As shown in Table 4, corrective

[11] SSA, POMS, DI 39566.010 A., *Disability Determination Services Physical Security*.

[12] The 122 deficiencies were identified during Security Reviews conducted at 9 DDSs in 9 regions in FYs 2005 and 2006. We did not visit Region II because there were few deficiencies reported at the Region's DDSs.

actions were not planned for 17 of the 20 deficiencies because the DDSs considered alternative controls were in place that were sufficient to ensure employees sensitive data and equipment were protected. Also, corrective actions were not planned for two deficiencies because the DDS did not consider it necessary since the DDS was planning to relocate the office. Additionally, one deficiency was not corrected because the DDS was not aware of SSA's retention requirements and did not consider corrective action necessary because it could rely on its Regional Office to provide documents not retained at the DDS.

Table 4: Corrective Actions Not Planned

Region	Location	Date Security Review Performed	Number of Corrective Actions	Reason Corrective Action is Not Planned
III	Roanoke, Virginia	February 2005	2	Relocation of DDS office planned.
IV	Raleigh, North Carolina	September 2006	5	DDS office stated it had alternative controls.
VI	Albuquerque, New Mexico	March 2005	1	DDS office was unaware of retention requirements.
VII	St. Louis (North), Missouri	September 2005	8	DDS office stated it had alternative controls.
IX	Carson City, Nevada	May 2005	4	DDS office stated it had alternative controls.
Total			**20**	

SSA policy stipulates both CDP and CSI will monitor the corrective actions until all weaknesses are corrected.[13] Joint responsibility is assigned because many of the actions necessary to accomplish corrective action involve both CSI and CDP.[14] However, the policy does not specify what duties each component is to perform in the monitoring process. We believe the lack of specific responsibilities for each component may create a risk that effective monitoring might not occur. SSA officials informed us that they are developing an automated system for the DDS Security Reviews that should alleviate the uncertainty about each regional component's responsibilities to monitor corrective actions and whether corrective actions have been taken.

[13] SSA, POMS, DI 39566.140 B.2.f., *DDS Compliance and Monitoring Procedures*.

[14] CDP has overall responsibility for the DDSs, and CSI has responsibility for oversight/monitoring of security.

Also, SSA policy does not require that CDP or CSI ensure DDS offices implement corrective actions within a specific timeframe. However, we found that SSA field offices[15] and the Office of Disability Adjudication and Review[16] are required to validate that corrective actions have been implemented within 90 days.

If deficiencies identified during Security Reviews are not resolved, there is a risk of unauthorized access to sensitive SSA information if DDS or SSA systems are compromised. Further, for the deficiencies related to the lack of Continuity of Operations Plans and Disaster Recovery Plans, a DDS may not be able to recover timely if a disaster impacts its facility. We believe SSA should clearly define the responsibilities, by component, for monitoring the progress of corrective actions taken on deficiencies identified during DDS Security Reviews to minimize risk to SSA and DDS information and systems. Establishing specific timeframes, such as 90-day intervals, for CDPs to contact DDS offices and validate that corrective actions have been implemented on all deficiencies identified during Security Reviews would ensure more timely resolution. As part of this resolution process, we believe SSA still needs to follow up on corrective actions for the 29 deficiencies we identified as unresolved to determine whether corrective actions are necessary.

UPDATE CHECKLIST FOR ADDITIONAL SECURITY CONCERNS

The DDS *Security Self-Review Checklist* that is used during the Security Review process did not address the new security concerns for protecting personally identifiable information (PII). Specifically, the checklist did not require that CSI determine whether laptop computers and related storage media are properly secured. A June 2006 message from the Chief Information Officer to all SSA employees, contractors and DDS employees gave examples of failures to protect PII, including "leaving an unprotected computer containing SSA information in a non-secure space" and "storing electronic files containing SSA information on a computer, flash drive, compact disc, etc. that other people can access."

---

[15] After a field office has received a final report on the findings and recommendations for corrective action, the field office manager has 45 days to develop a CAP to address any deficiencies noted in the final report. Also, the Area Director for the field office must validate the CAP within 90 days of receipt. For more information on the field office process, see our September 2007 audit, *Compliance with Onsite Security Control and Audit Review Requirements at Field Offices* (A-02-07-27021), page 2.

[16] After a hearing office has received an Onsite Security Control and Audit Review report, the hearing office manager has 30 calendar days to respond (either directly or through its regional office) with a report of the corrective actions planned and/or taken. Also, the office should forward, within 90 days of issuing the corrective action report, a validation report stating that corrective actions have been implemented. For more information on the hearing office process, see our September 2007 audit, *Onsite Security Control and Audit Review at Hearing Offices* (A-12-07-17080), page 2.

Also, the DDS *Security Self-Review Checklist* did not require that CSI address the following POMS security requirements.

- The computer room door is solid wood core.[17,18]
- Users lock or logoff the workstation or terminal prior to leaving it unattended.[19]

Such security weaknesses could result in a possible risk of unauthorized disclosure of sensitive SSA data as well as the loss of system hardware and software. SSA should update the DDS *Security Self-Review Checklist* to make it consistent with recent PII guidance and POMS security requirements.

CONCLUSION AND RECOMMENDATIONS

While we found the Security Review process for the DDS offices to be generally effective in both selecting DDSs for review and correcting identified deficiencies, improvements can be made to the Security Review process. We recommend SSA:

1. Ensure that regional CSIs review all DDS offices every 5 years or provide written justification if Security Reviews will not be performed.

2. Instruct regional CDPs and CSIs to obtain CAPs that address all deficiencies identified during Security Reviews within the 45-day timeframe from all DDS offices.

3. Consider revising the Agency's discretionary standards for protecting DDS facilities so that CAPs address all deficiencies identified during Security Reviews, even if the DDS position is that it will take no corrective action.

4. Clearly define the responsibilities, by component, for monitoring the progress of corrective actions taken on deficiencies identified during Security Reviews.

5. Establish specific timeframes, such as 90-day intervals, for CDPs to contact DDS offices and validate that corrective actions have been implemented on all deficiencies identified during Security Reviews.

6. Follow up on the 29 deficiencies we identified as unresolved to determine if corrective actions are necessary.

7. Update the DDS *Security Self-Review Checklist* to make it consistent with recent PII guidance and POMS security requirements.

---

[17] SSA, POMS, DI 39566.010 B.2.I., *DDS Physical Security.*

[18] Although the DDS *Security Self-Review Checklist* did not include a requirement to check with construction material of the computer room door, Region VII CSI noted that the computer room doors at the Missouri DDS did not meet the standards identified in POMS.

[19] SSA, POMS, DI 39566.001 C.14.b., *Scope of Privacy and Security Subchapter*.

AGENCY COMMENTS

SSA generally agreed with six of the seven recommendations and has begun taking corrective actions where possible (see Appendix C). However, SSA disagreed with our recommendation to consider revising the Agency's discretionary standards for protecting DDS facilities.

OIG RESPONSE

We agree with SSA that the intent of its DDS security policy is that CAPs should address all deficiencies identified during Security Reviews. For this reason, we still believe that SSA should consider revising its discretionary standards for protecting DDS facilities so that CAPs address all deficiencies identified during Security Reviews.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

CAP	Corrective Action Plan
CDP	Center for Disability Programs
CSI	Center for Security and Integrity
DDS	Disability Determination Services
DRP	Disaster Recovery Plan
FY	Fiscal Year
IDS	Intrusion Detection System
MCR	Management Control Review
PII	Personally Identifiable Information
POMS	Program Operations Manual System
SSA	Social Security Administration

Scope and Methodology

To accomplish our objective, we:

- Reviewed the Social Security Administration's (SSA) Management Control Review Program and related Federal requirements.
- Reviewed SSA policy and procedures, as well as prior Office of the Inspector General audits and other independent reviews, related to system and physical security at Disability Determination Services (DDS) offices.
- Contacted Center for Security and Integrity (CSI) staff in each of the 10 SSA regional offices to determine their methodology for selecting DDS offices for Security Reviews.
- Obtained data from CSI staff in each region to determine whether the DDSs were being reviewed in accordance with SSA's policies and procedures. We identified 89 Security Reviews conducted from October 1, 2001 through September 30, 2006.[1]
- Reviewed 32 Security Review reports issued from October 1, 2004 through September 30, 2006 to determine whether (1) CSI issued the report within 45 days from the date of the review and (2) the DDS provided a Corrective Action Plan within required 45 days.
- Reviewed the Security Reviews conducted between October 1, 2004 and September 30, 2006 and identified 225 deficiencies. We selected Security Reviews conducted at 9 DDS offices with 122 deficiencies.[2] We contacted relevant DDS/CSI personnel to verify appropriate corrective actions occurred.
- Reviewed the DDS *Security Self-Review Checklist* and solicited ideas from CSI and other SSA staff to identify additional steps SSA can take to enhance the Security Review process.

We found data used for this audit were sufficiently reliable to meet our objectives. The entities audited were SSA's Center for Security and Integrity and the Office of Disability Determinations, both under the Deputy Commissioner for Operations. We performed our audit in Kansas City, Missouri, and Chicago, Illinois, between October 2006 and August 2007 in accordance with generally accepted government auditing standards.

[1] There are 52 DDSs; however, several states have multiple DDS sites.

[2] We did not select a Security Review from Region II because there were few deficiencies reported in the Region's DDSs.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: January 15, 2008 Refer To: S1J-3

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

From: David V. Foster /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Compliance with Disability Determination Services Security Review Requirements" (A-05-07-17082)--INFORMATION

We appreciate OIG's efforts in conducting this review. Our response to the report findings and recommendations are attached.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "COMPLIANCE WITH DISABILITY DETERMINATION SERVICES SECURITY REVIEW REQUIREMENTS" (A-05-07-17082)

Thank you for the opportunity to review and provide comments on this draft report. We note that you generally found our procedures effective for selecting Disability Determination Services (DDS) offices and that we ensure correction of deficiencies that are identified through the security reviews. The draft report made suggested improvements to the security review process. For the most part, we agree with the recommendations, and have already begun taking corrective actions, where possible. However, several of the recommendations may require a change in policy and will involve more in-depth discussions before final decisions can be made.

Our responses to the specific recommendations are provided below:

Recommendation 1

Ensure that regional Centers for Security and Integrity (CSI) review all DDS offices every 5 years or provide written justification if Security Reviews will not be performed.

Comment

We agree. On December 28, 2007, we issued reminders to the CSIs to ensure that, where possible all DDSs are reviewed within the 5-year period. We also reminded them of the need for written justification when a review will not be performed.

Recommendation 2

Instruct regional Centers for Disability Programs (CDP) and CSIs to obtain corrective action plans (CAPs) that address all deficiencies identified during Security Reviews within the 45-day timeframe from all DDS offices.

Comment

We agree with the intent of the recommendation. The intent of the DDS security Program Operations Manual System (POMS) is that the CAPs should address all deficiencies identified during the review. Our POMS currently instructs the DDS to submit their CAPs to the regional office within 45 days after completion of the security review. The regional office is responsible for working with the DDSs to ensure that the CAP addresses all of the deficiencies. We will consider updating our POMS to emphasize the regional office oversight responsibilities.

Recommendation 3

Consider revising the Agency's discretionary standards for protecting DDS facilities so that CAPs address all deficiencies identified during Security Reviews, even if the DDS position is that it will take no corrective action.

Comment

We disagree. Some areas of POMS provide discretionary guidelines based on regulations found in 20 C.F.R. (Subpart Q). These regulations outline the basic responsibilities for SSA and the State.

Where a potential deficiency is cited that falls under the discretionary guidelines of POMS, we instruct the DDS to conduct a risk assessment to determine appropriate corrective action. The results of the risk assessment are considered part of the site's CAP. The regional CDP reviews the risk assessment to determine final outcome. Depending on the specific circumstances, the regional office may consult with the Office of Disability Determinations on whether the issue can be considered closed.

Recommendation 4

Clearly define the responsibilities, by component, for monitoring the progress of corrective actions taken on deficiencies identified during Security Reviews.

Comment

We agree with the intent of the recommendation. We will consider revising the DDS security POMS to clearly delineate the regional office oversight responsibilities. The draft POMS will need to be reviewed by the regional office and appropriate headquarters components for concurrence before implementing.

Recommendation 5

Establish specific timeframes, such as 90-day intervals, for CDPs to contact DDS offices and validate that corrective actions have been implemented on all deficiencies identified during Security Reviews.

Comment

We agree. We will revise the DDS security POMS to include instructions for providing follow-ups at 90-day intervals until all deficiencies have been addressed or risk assessments have been conducted and agreed on as an appropriate course of action.

Recommendation 6

Follow up on the 29 deficiencies we identified as unresolved to determine if corrective actions are necessary.

Comment

We agree. We have reviewed the 29 deficiencies and provided an update for each one. All of the deficiencies cited have been addressed and resolved and are now considered closed. A copy of the corrective actions has been provided under separate cover.

Recommendation 7

Update the DDS Security Self-Review Checklist to make it consistent with recent Personal Identifying Information (PII) guidance and POMS security requirements.

Comment

We agree. We will revise the DDS Security Self-Review Checklist to include current security guidance.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Walter Bayer, Director, Chicago Audit Division (312) 353-0331

Shannon Agee, Audit Manager, Kansas City Audit Division (816) 936-5590

Acknowledgments

In addition to those named above:

Tonya Coffelt, Senior Auditor

Elizabeth Juárez, Senior Auditor

Kim Beauchamp, Writer-Editor

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 Specialist at (410) 965-3218. Refer to Common Identification Number A-05-07-17082.

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 our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises 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 and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity 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 OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG 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. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.