OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

SINGLE AUDIT OF THE STATE OF MINNESOTA FOR THE FISCAL YEAR ENDED JUNE 30, 2000

February 2002 A-77-02-00009

AUDIT REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

Office of the Inspector General

MEMORANDUM

Date: FEB 27 2002

Refer To:

To: Ellen Baese
Director
Management Analysis and Audit Program Support Staff

From: Assistant Inspector General
for Audit

Subject: Single Audit of the State of Minnesota for the Fiscal Year Ended June 30, 2000 (A-77-02-00009)

This report presents the Social Security Administration's (SSA) portion of the single audit of the State of Minnesota for the Fiscal Year ended June 30, 2000. The Minnesota Legislative Auditor performed the audit. Results of the desk review conducted by the Department of Health and Human Services (HHS) have not been received. We will notify you when the results are received if HHS determines the audit did not meet Federal requirements.

The Minnesota Disability Determination Services (DDS) performs disability determinations under SSA's Disability Insurance (DI) and Supplemental Security Income (SSI) programs in accordance with Federal regulations. The DDS is reimbursed for 100 percent of allowable costs. The Minnesota Department of Economic Security (DES) is the Minnesota DDS's parent agency.[1]

For single audit purposes, the Office of Management and Budget assigns Federal programs a Catalog of Federal Domestic Assistance (CFDA) number. SSA's DI and SSI programs are identified by CFDA number 96. SSA is responsible for resolving single audit findings reported under this CFDA number.

The single audit reported the following findings (see Appendix A)

- Some DES employees had inappropriate access to mainframe data. The corrective action plan indicates that employee access is being reviewed and will be limited to employees with legitimate business needs.

- DES did not properly maintain its security infrastructure. The corrective action plan indicates that a system is now in place to properly maintain DES' databases.

[1] Organizationally, the DDS is under the Workforce Wage Assistance Branch within the Department of Economic Security.

We recommend that SSA ensure that the DDS:

1 Limits access to mainframe data to only those employees with legitimate business needs.

2. Has adequate systems security procedures in place for safeguarding claimant information.

The single audit also disclosed the following findings that may impact DDS operations, although they were not specifically identified to SSA. I am bringing these matters to your attention as they represent potentially serious service delivery and financial control problems for the Agency (see Appendix B).

- DES did not have procedures in place to adequately monitor manual checks
- The Department of Finance did not provide adequate direction to State agencies for certain types of financial transactions.

DES did not conduct independent quality control reviews of system batch jobs.

Computer controls were not in place at DES concerning employee access, accounts and passwords.

The Department of Administration did not have written security infrastructure procedures.

Please send copies of the final Audit Clearance Document to Mark Bailey in Kansas City and Paul Wood in Baltimore. If you have questions contact Mark Bailey at (816) 936-5591.

Paul H Wood for
Steven L. Schaeffer

Attachments

MINNESOTA OFFICE OF THE LEGISLATIVE AUDITOR
STATEWIDE SINGLE AUDIT
SCHEDULE OF FEDERAL PROGRAM AUDIT FINDINGS
FISCAL YEAR ENDED JUNE 30, 2000

CFDA NO.	PROGRAM NAME	STATE AGENCY	RPT NO.	FIND NO.	INT CONT	COMP REQ	PROBLEM	FIN IMPACT
U. S. Department of Justice								
16.540	Juvenile Justice & Delinquency Prevention	Economic Security	01-05	3		B	Questionable payment of board compensation	$9,515
U. S. Department of Labor								
17.207	Employment Services	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.207	Employment Services	Economic Security	01-07	1	RC	M	Inadequate oversight of program vendors	P
17.207	Employment Services	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.207	Employment Services	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.225	Unemployment (Reimployment) Insurance	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.225	Unemployment (Reimployment) Insurance	Economic Security	00-21	2	RC		Inappropriate clearance to scheuled batch jobs	P
17.225	Unemployment (Reimployment) Insurance	Economic Security	01-07	2	RC		Inadequate control over manual refund checks	P
17.225	Unemployment (Reimployment) Insurance	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.225	Unemployment (Reimployment) Insurance	Economic Security	00-21	4	RC		Inadequate controls of network accounts	P
17.246	Employment and Training Assistance	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.246	Employment and Training Assistance	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.246	Employment and Training Assistance	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.250	Job Training Partnership Act	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.250	Job Training Partnership Act	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.250	Job Training Partnership Act	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.253	Welfare to Work Program	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.253	Welfare to Work Program	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.253	Welfare to Work Program	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.801	Disabled Veterans Outreach Program	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.801	Disabled Veterans Outreach Program	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.801	Disabled Veterans Outreach Program	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
17.804	Local Veterans' Employment	Economic Security	00-21	1	RC		No quality control review for scheduled batch jobs	P
17.804	Local Veterans' Employment	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
17.804	Local Veterans' Employment	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
U. S. Social Security Administration								
96.001	Social Security Disability Insurance	Economic Security	00-21	2	RC		Inappropriate clearance to scheduled batch jobs	P
96.001	Social Security Disability Insurance	Economic Security	00-21	3	RC		Inadequate maintainence on security infrastructure	P
U. S. Department of Transportation								
20.205	Highway Planning & Construction	Transportation	01-13	1	RC		Noncompliance with state and federal guidelines	NQ

THE ATTACHED EXPLANATION IS AN INTEGRAL PART OF THIS SCHEDULE.

Department of Economic Security
Mainframe Scheduled Batch Processing
MIPS Accounting System

Conclusions

The department limited access to its scheduled batch environment. However, as discussed in Finding 1, some scheduled batch jobs were not subjected to an independent quality control review. Finding 2 discusses our concerns about some information system professionals with inappropriate clearance to the scheduled batch environment. Finally, in Finding 3, we discuss ACF2 maintenance issues that came to our attention.

1. Some scheduled batch jobs were not subjected to an independent quality control review.

During 1999, the department scheduled and ran over 300 batch jobs without first subjecting them to an independent quality control review. Referred to by the department as "ad hoc" or "fix" jobs, these jobs contain programs that will typically be used only once to accomplish a specific objective. These jobs accounted for less than one percent of the scheduled batch activity during 1999. Currently, a programmer who develops one of these jobs must submit a Fix/ADHOC Job Run Request form to the Data Control Unit. Data Control then uses this information to schedule and run the job. Throughout this process, no independent person reviews the propriety of the job contents.

It is important to independently review scheduled batch jobs because they are inherently risky. Scheduled batch jobs typically have very powerful security clearances and do not require passwords. The introduction of an unauthorized or improperly coded scheduled batch job could lead to a disastrous loss or the widespread destruction of critical business data.

Recommendation

- *The department should independently review all scheduled batch jobs.*

2. Some information system professionals have inappropriate clearance to the scheduled batch environment.

Some information system professionals with access to the scheduled batch environment do not need this clearance to fulfill their regular job duties. We found groups of computer operations, help desk, and telecommunications employees who had complete and unfettered access to critical components of the scheduled batch environment. We also found two former employees with complete access. One of these former employees never used his account to access the mainframe and the other last used her account in November 1998.

We recognize that there are occasions when employees outside the Data Control Unit may need access to the scheduled batch environment. However, granting large groups of people complete and continuous access to sensitive batch job data exposes the department to unnecessary business risks.

Recommendations

- *The department should limit access to the scheduled batch environment to only those people who need that access to fulfill their normal job duties.*

- *The department should develop special scheduled batch environment access procedures for those employees outside the Data Control Unit.*

3. The department did not perform necessary maintenance on its ACF2 security infrastructure.

We found many obsolete ACF2 security rules and user accounts during our review of scheduled batch processing. Maintaining the ACF2 security databases is an important security administration responsibility. When left uncontrolled, inactive accounts and unneeded security rules can provide intruders with access to critical business data.

We identified these same weaknesses in our audit report released in March 1998. In response to this issue, the department purchased software to streamline ACF2 maintenance. However, security officers have not used this software since 1998.

Recommendations

- *The department should periodically cancel or suspend user accounts that are no longer needed.*

- *The department should periodically purge unneeded security rules from the ACF2 security database.*

State of Minnesota
Department of Economic Security

390 North Robert Street
Saint Paul, Minnesota 55101

Office of the Commissioner

May 8, 2000

Mr. James R. Nobles
Legislative Auditor
First Floor, Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

The following information is offered in response to your draft audit report for the period ended February 29, 2000.

Conclusion:

1. **Some scheduled batch jobs were not subjected to an independent quality control review.**

Response:
We agree. The Department of Economic Security will revise it's policy regarding the running of "fix" and "ad hoc" jobs to require the approval of the programming supervisors responsible for the specific job or program effected. A paper copy of the "fix" or "ad hoc" job request will be retained in the Data Control unit. Following the entry on the security log a data security administrator will review the paper request to ensure that all required approvals were obtained prior to the jobs being run.

Responsible Individual: Mark Butala

Conclusion:

2. **Some information system professionals have inappropriate clearance to the scheduled batch environment.**

Response:
We agree. Only individuals who have a business reason should have access to the scheduled batch environment. Scheduled batch job access was recently deleted for the two former employees. Data security staff will meet with the supervisors of employees who currently have access. Together, the batch environment software supervisor, the security administrator and business unit supervisors will determine which individuals have a legitimate business need, all others will have their access deleted.

Responsible Individual: Mark Butala

James Nobles
Page Two
May 8, 2000

Conclusion:

3. The department did not perform necessary maintenance on its ACF2 security infrastructure.

Response:
We agree. Beginning in February 2000 a computer job was implemented and will continue to be run monthly. The job will cancel all user logons that have not been accessed within a 90-day period. Also, the same job will cancel any logon that has not been accessed since being established or since the last time a data security administrator changed the password.
Since April 2000 the data security administrators have used ETF/A software for maintaining its ACF2 databases. Currently dataset rules and resource rules through the fourth quarter of 1999 have been purged. Security staff will continue to keep these databases current.

Responsible Individual: Mark Butala.

Conclusion:

4. The department did not adequately control some powerful network accounts.

Response:
We agree. The Department of Economic Security will review all Novell Network accounts to insure that all user passwords will expire on a routine basis. We will also review the use of shared accounts and determine the appropriateness of their use. Particular attention will be paid to accounts with powerful rights and privileges and wherever possible individual, unique accounts will be created or additional layers of access controls will be implemented.

Responsible Individual: Mark Butala

Sincerely,

Earl R Wilson

Earl R. Wilson
Commissioner

Department of Economic Security

2. The Department of Economic Security did not adequately monitor manual checks.

The department did not adequately monitor certain manual checks generated from the Unemployment Insurance Benefit Account. The checks are primarily used to return funds when applicants have overpaid the department. During fiscal year 2000, we noted that the department produced 157 checks totaling $488,000. The department also issued manual checks to transfer funds to other state agencies and to other accounts within the department; however, they now make these transfers electronically. We noted a key weakness with the department's internal controls for processing manual checks. One employee was responsible for preparing and mailing the checks, as well as recording the transactions in the accounting system. These functions are typically incompatible. The department has not developed any mitigating controls to monitor these sensitive checks. To reduce the risk of unauthorized transactions, someone independent of this process should ensure that all checks issued were properly authorized.

Recommendation

- *The Department of Economic Security should improve internal control by having an independent person review manual checks issued from the Unemployment Insurance Benefit Account to ensure that all checks issued were authorized.*

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Economic Security. This restriction is not intended to limit the distribution of this report, which was released as a public document on March 8, 2001.

James R. Nobles
James R. Nobles
Legislative Auditor

Claudia J. Gudvangen
Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: January 25, 2001

Report Signed On: March 5, 2001

Department of Finance

1. The Department of Finance did not make entries in the accounting system to move cash from the state's General Fund to the Minnesota State College and University system's fund.

Although the Department of Finance established appropriations and spending authority in the Minnesota State Colleges and Universities (MnSCU) Fund for certain capital projects, it did not adjust the accounting system to move cash totaling $51,300,000 from the state's General Fund to the MnSCU Fund. The Legislature made the appropriations during the 1997 legislative session ($9,300,000), the 1999 legislative session ($36,200,000), and the 2000 legislative session (5,800,000).

The state depends on the accounting system as an accurate record of the state's financial activity. Until the Department of Finance made the correcting entries in November 2000, the accounting system overstated the state's General Fund cash balance by $51,300,000 and understated MnSCU's General Fund cash balance by the same amount. The oversight did not affect the investment of the cash or inhibit MnSCU's ability to proceed with the capital projects funded by the appropriations. Since these funds are combined for financial statement presentation, the error did not result in a financial statement misstatement.

Recommendation

- *The Department of Finance should ensure that it records cash in the proper funds on the state's accounting system.*

2. The Department of Finance did not provide state agencies with adequate direction for certain types of transactions to ensure that the state's financial statements properly present this financial activity.

The Department of Finance could provide better guidance to agencies for the following situations:

- Advance Grants – Although the state provides most grant funds on a reimbursement basis, it provides some funds in advance of subrecipient expenditures. For example, the Department of Natural Resources advanced money to some organizations for flood control projects. In its financial statements, the state should recognize expenditures equal to the amount subrecipients expended during the fiscal year. The state should show any unspent advances as prepaid expenses. State agency staff may not be aware that they need this information for proper financial reporting. The agencies also may have to revise subgrantee reporting requirements in order to obtain this information from subgrantees.

- Multi-year projects – The time frame of some of the state's projects may span several fiscal years, even several bienniums. Financial reporting problems may occur when agencies encumber funds for project costs that they will pay with dedicated revenue collected in subsequent years. Agencies are uncertain what portion, if any, of the encumbrance amount to show as reserved fund balance. Reserving the entire encumbrance amount may result in a negative fund balance, which agencies may be hesitant to report. Consequently, some agencies have underreported encumbrances.

These types of transactions are at a greater risk of financial reporting errors since agency staff may not be aware of the applicable accounting principles related to them. Although errors related to this financial activity have not posed a significant risk, these situations do recur each year and may be more significant in future years. By providing guidance for these concerns now, the department may prevent a material error in the future.

The Department of Finance could also improve its annual requests to agencies for financial statement information. Some requests consistently result in data that financial reporting staff has to further refine or that is not traceable back to the state's accounting system. The department should solicit information about any new types of transactions or initiatives the agencies have undertaken during the fiscal year so that financial reporting staff can determine the financial statement impact of that activity. Also, requests should include the dates by which the department needs the requested data.

Recommendations

- *The Department of Finance should provide state agencies with guidance in the proper financial statement presentation of advance grant transactions and multi-year projects.*

- *The Department of Finance should review its annual requests for agency financial statement data and make revisions to improve the quality of the data submitted.*

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Finance. This restriction is not intended to limit the distribution of this report, which was released as a public document on March 15, 2001.

James R. Nobles
James R. Nobles
Legislative Auditor

Claudia J. Gudvangen
Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: January 26, 2001

Report Signed On: March 12, 2001

Department of Economic Security
Mainframe Scheduled Batch Processing
MIPS Accounting System

Conclusions

The department limited access to its scheduled batch environment. However, as discussed in Finding 1, some scheduled batch jobs were not subjected to an independent quality control review. Finding 2 discusses our concerns about some information system professionals with inappropriate clearance to the scheduled batch environment. Finally, in Finding 3, we discuss ACF2 maintenance issues that came to our attention.

1. Some scheduled batch jobs were not subjected to an independent quality control review.

During 1999, the department scheduled and ran over 300 batch jobs without first subjecting them to an independent quality control review. Referred to by the department as "ad hoc" or "fix" jobs, these jobs contain programs that will typically be used only once to accomplish a specific objective. These jobs accounted for less than one percent of the scheduled batch activity during 1999. Currently, a programmer who develops one of these jobs must submit a Fix/ADHOC Job Run Request form to the Data Control Unit. Data Control then uses this information to schedule and run the job. Throughout this process, no independent person reviews the propriety of the job contents.

It is important to independently review scheduled batch jobs because they are inherently risky. Scheduled batch jobs typically have very powerful security clearances and do not require passwords. The introduction of an unauthorized or improperly coded scheduled batch job could lead to a disastrous loss or the widespread destruction of critical business data.

Recommendation

- *The department should independently review all scheduled batch jobs.*

2. Some information system professionals have inappropriate clearance to the scheduled batch environment.

Some information system professionals with access to the scheduled batch environment do not need this clearance to fulfill their regular job duties. We found groups of computer operations, help desk, and telecommunications employees who had complete and unfettered access to critical components of the scheduled batch environment. We also found two former employees with complete access. One of these former employees never used his account to access the mainframe and the other last used her account in November 1998.

We recognize that there are occasions when employees outside the Data Control Unit may need access to the scheduled batch environment. However, granting large groups of

Department of Economic Security
Mainframe Scheduled Batch Processing
MIPS Accounting System

Conclusion

The department limited access to MIPS screens to only those employees who need access to fulfill their job duties. The department also limited the number of people who can update or delete MIPS data without using the intended screens. However, we found some network security weaknesses that could diminish the effectiveness of the MIPS data integrity controls. Finding 4 discusses these weaknesses in more detail.

4. The department did not adequately control some powerful network accounts.

During our audit, we found one powerful network account that was being shared by 13 people. This account had complete and unfettered access to most data on the department-wide network. This powerful network account, as well as eight other powerful network accounts, also did not require periodic password changes.

Creating unique accounts and passwords for all people is an important control because it ensures individual accountability. When people share accounts, it becomes nearly impossible to trace specific actions to individuals. Sharing accounts with powerful security clearances is particularly risky. In fact, it exposes the entire department to significant and unnecessary risks.

Enforcing periodic password changes is also an important control. Computers use passwords to authenticate the identity of specific people. Unfortunately, computerized tools now permit unscrupulous people to guess passwords. Enforcing periodic password changes minimizes this risk.

Recommendation

- *The department should create unique accounts for all people and enforce periodic password changes.*

Department of Administration
Intertechnologies Group
System-wide Access to Mainframe Data

1. ACF2 rules give many Intertech employees and installed software products widespread access to data.

Most ACF2 security rules grant large groups of Intertech information system professionals and installed software products complete and unfettered access to data. This data includes agency business data, files and programs essential to the mainframe computer's operating system, and even some ACF2 security data. We recognize that some people and software products need this type of broad access to perform ongoing system maintenance. However, we feel that most could fulfill their typical job duties with more targeted security clearances.

Of particular concern, we found many accounts with clearance to modify "authorized programs." Authorized programs are computer programs that reside in specially defined libraries. Access to these programs and libraries should be tightly controlled because they can be used to circumvent security. We also found an excessive number of accounts with clearance to modify critical operating system components. Normally, only a select few information system professionals with special skills need clearance to modify operating system parameters.

Writing security rules that give large groups of people and software products widespread and continuous access to data exposes the state to significant risks. When questioned, security officers at Intertech told us that they shared our concerns and were actively searching for solutions. These security officers told us that they were currently redefining the membership in existing security groups to make them more concise. They also were exploring ways to only give people temporary access to data, and then revoke that access when no longer needed. However, Intertech security officers had not implemented either of these solutions by the time we completed our work.

Recommendations

- *Intertech should define ACF2 security groups that are appropriate for specific job functions.*

- *Intertech should evaluate the need for powerful group clearances permitted in ACF2 security rules.*

2. Intertech did not adequately control some powerful ACF2 privileges.

Intertech did not implement important mitigating controls for some personal and software product accounts with powerful ACF2 privileges. One ACF2 privilege that we reviewed gives accounts the ability to access data without supplying a password. This privilege provides organizations with a mechanism to schedule and run computer job streams at night. Recognizing the risks posed by accounts with no passwords, the developers of ACF2 designed special compensating controls for security officers to deploy. However, we found many of these privileged accounts on the central mainframe computers at Intertech that did not utilize these important compensating controls. Some of these accounts held other powerful ACF2 privileges as well, compounding the risks even further. When questioned, Intertech told us that they created many of these powerful accounts before they fully understood how the compensating controls worked.

We also found some people with other powerful privileges that they may not need to fulfill their normal job duties. For example, one person we tested had clearance to access ACF2 to create or modify accounts. When questioned, this person did not realize that he had this clearance. Other people that we reviewed had inappropriate clearances to view ACF2 security rules. Finally, we found one person with inappropriate access to the most powerful ACF2 privilege. This is the privilege that identifies a person as an ACF2 security officer.

Recommendations

- *Intertech should deploy the ACF2 recommended compensating controls over all accounts that do not require passwords.*
- *Intertech should remove powerful ACF2 privileges from those people who do not need those privileges.*

3. One ACF2 exit may expose data to unauthorized access.

Intertech deployed an "exit" that permits access to any data that is not protected by an ACF2 rule. Organizations that install ACF2 can program their own exits to circumvent the security software's standard decision-making process. Normally, ACF2 does not permit a person or an installed software product to access data unless a security officer explicitly authorizes that access in a rule. Fortunately, Intertech has ACF2 rules that protect most critical business data on the central mainframe computers. Furthermore, this exit permits "read-only" access to all remaining unprotected data. However, when questioned, Intertech was unable to justify the need for this exit that bypasses ACF2's normal decision-making process.

Recommendation

- *Intertech should discontinue using the exit that allows read-only access to all data that is not secured by rules.*

4. Documentation of key components of the ACF2 security infrastructure is inadequate.

Intertech prepares very little written documentation for the ACF2 security infrastructure. This makes identifying the purpose of and technical contact for specific security rules quite difficult. It also makes it difficult to scrutinize the appropriateness of rules. For example, during our audit, we found some security rules that granted access to every mainframe account. Security officers told us that they could not answer our questions about the propriety of these rules without first doing an extensive amount of research to identify what the rule was intended to protect. Other information system professionals at Intertech were also unable to explain why these rules were needed.

Intertech has a very complex security infrastructure that contains over 60,000 ACF2 security rules. Without written documentation, challenging the appropriateness of individual security rules becomes extremely laborious. Inadequate documentation also could increase the time needed to recover business operations from a disaster.

Recommendation

- *Intertech and state agency security officers should develop written documentation for the ACF2 security infrastructure to facilitate security administration duties.*

Overview of the Office of the Inspector General

Office of Audit

The Office of Audit (OA) conducts comprehensive financial and performance audits of the Social Security Administration's (SSA) programs and makes recommendations to ensure that program objectives are achieved effectively and efficiently. Financial audits, required by the Chief Financial Officers Act of 1990, assess whether SSA's financial statements fairly present the Agency's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs. OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress, and the general public. Evaluations often focus on identifying and recommending ways to prevent and minimize program fraud and inefficiency.

Office of Executive Operations

The Office of Executive Operations (OEO) provides four functions for the Office of the Inspector General (OIG) – administrative support, strategic planning, quality assurance, and public affairs. OEO supports the OIG components by providing information resources management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this Office coordinates and is responsible for the OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act. The quality assurance division performs internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from the Agency. This division also conducts employee investigations within OIG. The public affairs team communicates OIG's planned and current activities and the results to the Commissioner and Congress, as well as other entities.

Office of Investigations

The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and by SSA employees in the performance of their duties. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Counsel to the Inspector General

The Counsel to the Inspector General provides legal advice and counsel to the Inspector General on various matters, including: 1) statutes, regulations, legislation, and policy directives governing the administration of SSA's programs; 2) investigative procedures and techniques; and 3) legal implications and conclusions to be drawn from audit and investigative material produced by the OIG. The Counsel's office also administers the civil monetary penalty program.