

OFFICE OF THE
INSPECTOR GENERAL



**MANAGEMENT ADVISORY REPORT
ADMINISTRATION OF TOP SECRET AT THE
NATIONAL COMPUTER CENTER**

**-- WARNING --
THIS REPORT CONTAINS RESTRICTED
INFORMATION FOR OFFICIAL USE.
DISTRIBUTION LIMITED TO AUTHORIZED
OFFICIALS.**

James G. Huse, Jr. – INSPECTOR GENERAL

September 2000

A-14-99-11001



SOCIAL SECURITY

MEMORANDUM

Office of the Inspector General

Date: SEP 15 2000

Refer To:

To: William A. Halter
Deputy Commissioner
of Social Security

From: Inspector General

Subject: Management Advisory Report – Administration of TOP SECRET at the National
Computer Center (A-14-99-11001)

THIS REPORT CONTAINS INFORMATION THAT IS SENSITIVE AND CONFIDENTIAL. FOR SECURITY REASONS, WE RECOMMEND THAT DISTRIBUTION OF THIS REPORT BE LIMITED TO THOSE WITH A NEED TO KNOW

OBJECTIVE

This Management Advisory Report presents the results of our evaluation of the Social Security Administration's (SSA) TOP SECRET access control software. The objective of our review was to examine the administration of TOP SECRET software to restrict unauthorized access to SSA's mainframe systems at the National Computer Center.

BACKGROUND

We initiated this review to continue prior work performed in this area. Our March 1997 report, *Review of CA-TOP SECRET Access Control Software*, recommended the Agency perform periodic reviews of the TOP SECRET options. In the *Social Security Administration Accountability Report for Fiscal Year 1998*, PricewaterhouseCoopers reported that SSA needed to improve mainframe security monitoring practices.

Agency managers are responsible for implementing and maintaining management controls that, among other things, reasonably ensure that Agency resources are protected from waste, fraud, and mismanagement. Controls can be preventive, corrective, or detective in nature. If one of these controls is weak, another must be strengthened to compensate for that weakness. System access controls, when implemented effectively, can prevent unauthorized individuals from accessing sensitive automated information. Access controls not only limit the quantity of system users, they establish user accountability within the system.

Systems managers are concerned about external intruders as well as internal breaches of access controls. The computer security industry identifies external intruders as well as a company's employees as a high-risk group with the potential to compromise the company's automated information systems.

SSA's TOP SECRET access control software package, when properly administered and maintained, limits access to SSA's mainframe critical and sensitive computer resources (data and programs) and mitigates the risk of accidental or intentional compromise of Agency information caused by unauthorized personnel access.

Strong access controls are critical to SSA because of the volume and nature of the transactions the Agency processes. SSA processes an average of 20 million program transactions per day. In Fiscal Year 1998, SSA issued benefits exceeding \$390 billion to over 50 million beneficiaries. SSA's computer systems support processing and storage of sensitive information, such as earnings records for clients, beneficiary and recipient claims records, and post-entitlement action records as well as Agency administrative functions. The Privacy Act of 1974 requires Federal agencies to protect the confidentiality and integrity of sensitive Federal information, such as the beneficiary data maintained in SSA's automated systems. Office of Management and Budget Circular A-130, appendix III, *Security of Federal Automated Information Resources*, which implements the Computer Security Act of 1987, requires technical security measures (such as access controls) for systems and review of system security controls at least every 3 years. The National Institute of Standards and Technology (NIST) provides guidance for system access controls in NIST Special Publications 800-12, *An Introduction to Computer Security: The NIST Handbook*, and 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*.

NIST Special Publication 800-14 states that identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user identification. NIST requires that inactive user identifications on the system for a specific period of time (for example, 3 months) be disabled. The Federal Information Systems Audit Manual recommends temporary user identification and authentication devices, such as passwords, be designed to automatically expire after a designated date.

Two major components within SSA administer TOP SECRET. The Office of Information Systems Security (OISS) is located in the Office of Financial Policy and Operations within the Office of the Deputy Commissioner for Finance, Assessment and Management. The SSA Systems Security Officer (SSASSO) interprets, develops, and implements SSA's systems security policy for TOP SECRET. Secondly, the Office of Telecommunications and Systems Operations within the Office of the Deputy Commissioner for Systems implements SSASSO's TOP SECRET policy, maintains the access control system, and reports security problems to the SSASSO for necessary action.

The TOP SECRET software establishes accessor identification (ACID) for each user. The system uses the ACID to authenticate the user. A user may have a unique six-digit personal identification number and a special ACID (commonly known as \$userids). Programmers use special ACIDs to access Office of Systems Operations systems. SSA's *Systems Security Handbook*, issued by OISS, contains two principles that guide access to SSA systems: (1) need to know and (2) least privilege. A need to know limits

access to only those users who have a legitimate need for the resource to perform their job duties. Least privilege restricts users' access to the minimum amount of capability necessary to perform their job functions (for example, program A but not B, read only or change/update).

SCOPE AND METHODOLOGY

To determine whether the administration of TOP SECRET limits access to SSA's mainframe computer resources according to the need to know and least privilege principles, we:

- reviewed SSA's configuration and use of the TOP SECRET access control software product;
- interviewed SSA's Office of Systems and Office of Systems Security staffs on the administration of TOP SECRET in the National Computer Center;
- reviewed the *Systems Security Handbook* to determine pertinent operating and security policies and procedures;
- examined SSA's systems security controls options and the quantity of special access accounts administered by SSA;
- examined TOP SECRET reports including the *Audit Utility Cross-Reference of Privileges and Attributes* report as of December 21, 1998;
- used non-statistical sampling to analyze other listings that disclosed selected control settings (see Appendix A);
- reviewed applicable laws, regulations, and publications including the Privacy Act of 1974, the Computer Security Act of 1987, Office of Management and Budget Circular A-130, and NIST Special Publications 800-12 and 800-14;
- examined manuals and technical guides for proper administration of access control software in the Federal Information Systems Audit Manual and the CA-TOP SECRET Auditor's Guide; and
- reviewed best business practices regarding proper management of an entity's central security control software in the Ernst and Young, Audit, Control, and Security of CA-TOP SECRET Technical Reference and the General Accounting Office CA-TOP SECRET Practice Aid (see Appendix B). The Practice Aid is adapted from Ernst and Young's Technical Reference manual.

We performed field work at SSA Headquarters and the National Computer Center in Baltimore, Maryland, between October 1998 and December 1999.

RESULTS OF REVIEW

We identified two major areas that warrant management's attention. The issues relate to the application of TOP SECRET controls and the need to review TOP SECRET controls to detect unauthorized access. To effectively administer the TOP SECRET access control software, we believe SSA must address the conditions identified below.

APPLICATION OF TOP SECRET CONTROLS

In our review of the application of TOP SECRET controls, we found two conditions exist: excessive special access accounts and inappropriate authority granted.

Excessive Special Access Accounts

SSA had 96 ACIDs with control permission to access SSA's mainframe environment. The 96 ACIDs had the highest access authority, which allowed them to override any or all security features specified for SSA's mainframe systems. In January 1999, we monitored 30 of the 96 ACIDs to see how often they employed their highest-level access authorities. We found 16 of the 30 ACIDs access the system daily, and 14 ACIDs we reviewed did not access SSA's systems daily. We identified one active ACID that had not been used since June 1998. SSA has no policy to monitor the use of those ACIDs with access to sensitive resources, such as the ability to add and remove ACIDs from the systems security database. An intruder could compromise the active ACID and create an ACID with powerful access that bypasses established security features.

SSA does not have predetermined time periods for terminating temporary and seldom-used ACIDs, such as contract auditors' ACIDs. Of the 30 ACIDs we examined, 4 belonged to contract auditors and were inactive. The auditors were granted authority to read system control settings. Confidential system settings are subject to exposure through these inactive ACIDs with high-level security privileges that can be activated by the flip of a switch. SSA has no policy to delete inactive ACIDs or establish temporary access authorization (that is, ACIDs are automatically terminated after a given period) to prevent an individual from compromising an inactive ACID thereby corrupting sensitive agency information.

Inappropriate Authority Granted

In addition, SSA had 254 ACIDs in December 1998 with special privileges access authority to use SSA's mainframe system security controls. We identified 210 ACIDs with CONSOLE privileges¹ that enable an individual to change system-incorporated control options, 73 ACIDs with the ability to make new password changes,² and

¹ CONSOLE privileges allow individuals to execute started tasks (started tasks in privileged status bypass all TOP SECRET authorization processing) or change security control options.

² New password change privileges allow individuals to customize password security rules.

29 ACIDs with the ability to bypass existent security control procedures. These 29 ACIDs are available for emergency processing, for example, if a critical program terminates during the night. The operator asks for an emergency bypass account that allows him to input the necessary changes for the job to continue processing. We determined that 10 of the 29 ACIDs had not been used since July 1998. SSA has no policy to review the use of the special privileges ACIDs and delete idle ACIDs with access authority, such as CONSOLE privileges, emergency bypass access, and new password change authority. As a result of these vulnerabilities, an individual could change the TOP SECRET's security structure, for example create new password rules, to possibly gain access to sensitive information.

STRENGTHEN REVIEW OF CONTROLS TO DETECT UNAUTHORIZED ACCESS

SSA established a mainframe security monitoring system through the development of the Security Management Action Report (SMART). SMART summarizes the daily violation reports of inappropriate activity on SSA's mainframe systems over a period of time. OISS designed SMART to focus management's attention on a specific type of transaction scenario, so the Agency can obtain useful target and trend information.

According to PricewaterhouseCoopers,³ SSA lacks active monitoring controls over SMART. Without adequate review of these violation detection reports, the daily TOP SECRET access violation reports or the SMART, we believe unauthorized accesses for the commission of fraud may not be detected in a timely manner.

SSA needs to regularly review systems programmers' access. SSA's *Systems Security Handbook* requires SSA component managers to review systems programmer access privileges to enforce the need to know and the least privilege concepts. According to the 1999 CSI/FBI *Computer Crime and Security Survey*,⁴ employees account for 55 percent of the reported unauthorized access incidents. SSA developed a standardized profile team to assist in implementing the standardized access profiles for computer programmers in each component. However, even with the use of standardized profiles, SSA still needs to regularly review the employee's access. We examined 20 authorized program facility libraries that contained critical system programs. Of the 20 libraries, we identified 1 library with 17 ACIDs registered as having the change capability to the library. The remaining 19 authorized program facility libraries had on average 5.8 ACIDs with change capabilities. System programmers are the system's greatest asset and liability with respect to potential system security threats. The greatest single exposure from programmer access is update authority to the

³ *Social Security Administration Accountability Report for Fiscal Year 1999*, PricewaterhouseCoopers, November 1999.

⁴ Source: Richard Power. 1999 CSI/FBI *Computer Crime and Security Survey*. *Computer Security Issues and Trends V*, 1 (winter 1999).

authorized program facility libraries. A programmer could easily corrupt critical system programs thereby damaging sensitive agency information.

CONCLUSIONS AND RECOMMENDATIONS

We believe SSA management needs to strengthen its administrative controls for safeguarding sensitive information stored on its systems. The Agency needs to ensure access is granted consistent with the least privilege concept and regularly review inactive ACIDs and report on unauthorized access. According to best practices (Appendix B), SSA needs to limit administrator access and special privileges capabilities, such as the ability to change installation options, access the security data base, alter ACIDs and passwords, and bypass system security settings. SSA needs to continually review violation reports and critical employee access. Specifically, SSA should:

1. review employee job functions annually and access privileges to minimize the number of security control ACIDs and special privilege ACIDs in the TOP SECRET environment;
2. remove inactive ACIDs from the TOP SECRET security file;
3. establish a procedure to monitor and document periodic reviews of access violation reports to detect access compromises in a timely manner;
4. establish a procedure to perform continuous reviews of Terminal Sharing Options users access privileges in accordance with the least privilege concept; and
5. establish policy and procedures to automatically remove inactive ACIDs.

AGENCY COMMENTS

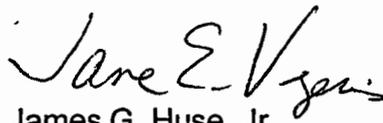
In response to our draft report, SSA agreed with the intent of our five recommendations but is unwilling to implement Recommendations 1, 2 and 5. For Recommendation 1, SSA stated that review of employee job functions and systems access is ongoing, with its frequency depending on system changes. SSA also stated that ongoing and periodic evaluations of Agency personnel systems access is based on the least privilege concept.

While agreeing with the intent of Recommendations 2 and 5, SSA stated the recommendations were not feasible. SSA cannot remove the inactive ACIDs from the security file because software used to audit the file would fail. SSA has addressed or will have addressed Recommendations 3 and 4 by December 2000.

OIG RESPONSE

We agree with SSA's plan to issue a memorandum by the end of Fiscal Year 2000 reminding Agency components of the need to continually review job functions and systems access. However, SSA should issue this memorandum annually to reinforce those review requirements. By reminding components to review employee job functions and access privileges annually, specifically the security control and special privilege ACIDs in the TOP SECRET environment, SSA reduces unauthorized access to sensitive information.

We continue to recommend removal of inactive ACIDs from the security file. SSA should consider modifying the audit software utility to accept the elimination of ACIDs. According to a survey by the Computer Security Institute and the Federal Bureau of Investigations⁵, losses from cybercrime are growing. Hackers are becoming more sophisticated. They could hack into SSA's mainframe system, reactivate a security control ACID, and obtain the highest privileges to access SSA's most sensitive information. This risk of unauthorized access is even greater for internal users, employees who already have access to, and knowledge of, SSA systems. SSA needs to purge the security file of inactive ACIDs to maintain strong systems security.


for James G. Huse, Jr.

⁵ Source: Marcia Savage. *Cybercrime on the Rise*. *Computer Reseller News* (July 31, 2000).

Appendices

Appendix A – Non-statistical Sampling

Appendix B – Best Practices

Appendix C – SSA Comments

Appendix D – OIG Contacts and Staff Acknowledgements

Non-statistical Sampling

1. We selected 41 control accessor identification (ACID) administrators consisting of:

- 1 Master Security Control ACID,
- 10 Central Security Control ACIDs,
- 10 Zone Security Control ACIDs,
- 10 Divisional Security Control ACIDs, and
- 10 Departmental Security Control ACIDs.

We examined the 41 Control ACIDs' security control settings and their associated scope of authority.

2. We examined 30 of the 96 Security Control ACIDs for the last used date by querying all mainframe systems.
3. We examined 20 started task ACIDs and 20 authorized program facility ACIDs for appropriate execute and update capabilities.

Best Practices

We reviewed the Ernst and Young, Audit, Control, and Security of CA-TOP SECRET Technical reference and the General Accounting Office CA-TOP SECRET Practice Aid for the best practice procedures on proper management of an entity's central security software. We have listed below our review of the following TOP SECRET control areas: yes, we found proper controls within that control area or no, we did not find proper controls within that control area.

TOP SECRET CONTROL AREAS	REVIEW RESULTS
Administrative Controls	
1. Installation Options	Yes
2. Security Data Base Access	No
3. Installation Exits	Yes
4. Bypass Control	No
Assigning Access and Granting Authorities	
5. Special Privileges	No
6. System Access	No
7. ALL	No
8. Password Administration	No
9. Batch Jobs	Yes
10. Started Procedures Table	No
11. Subsystem Interface	Yes
12. Access Levels	No
13. Higher Levels	No
Reporting and Reviewing Violations	
14. Logging	No

The Social Security Administration (SSA) needs to limit access to the security data base and the bypass control ACIDs. Secondly, SSA needs to restrict authorization capabilities with special privileges, system access, various access levels including high level access, and the ALL access. We also discovered the need to control access to SSA facilities through the limitation of password change capabilities and of access within started procedures table. The last TOP SECRET control area that needs improvement is the review of logging reports of system access violations.



SOCIAL SECURITY

MEMORANDUM

Date: August 22, 2000

Refer To:

To: James G. Huse, Jr.
Inspector General

From: William A. Halter *WAH*
Deputy Commissioner of Social Security

Subject: The Office of the Inspector General Draft Report,
"Administration of TOP SECRET at the National Computer Center"
(A-14-99-11001)--INFORMATION

Our comments on this report are attached. If your staff have any questions, they may contact Mark Welch on extension 50374.

Attachment
SSA Response

Agency Comments

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "ADMINISTRATION OF TOP SECRET AT THE NATIONAL COMPUTER CENTER" (A-14-99-11001)

Thank you for the opportunity to review and provide comments on this OIG draft report. During and since the time that this OIG audit was conducted (October 1998 through December 1999), SSA has taken many steps to strengthen mainframe computer security and keep ahead of emerging threats. Consequently, some of the conditions and findings noted in this report are not indicative of today's environment.

For example, the report (page 5) indicates that 210 accessor identifications (ACID) with special privilege access authority also had CONSOLE privileges (which allow modification of security control options). Today, the number is 113, and all are sanctioned by the Social Security Administration (SSA) Information Systems Security Officer (SSAISSO). Of those ACIDs with CONSOLE privileges, 30 are assigned to employees executing SSA's batch emergency procedure and are limited to basic CONSOLE permissions. That is, these ACIDs are not associated with any facilities, thus preventing a log-on to any mainframe system or performance of other administrative duties. Seventeen ACIDs are assigned to the SSA Office of System's Central Security Administrators to manage and control CA-TOP SECRET security software. Without this authority, SSA would be left without backup coverage capabilities should a disaster occur. Sixty-six ACIDs are assigned to physical Multiple Virtual Storage system consoles, are not associated with any facilities and cannot be used to log-on to any mainframe computer system. These consoles require the CONSOLE attribute to maintain and respond to the TOP SECRET security system for operational management of the product.

The report also indicates (page 4) that SSA does not have predetermined time periods for terminating temporary and seldom used ACIDs. However, we now have approved security policy for terminating temporary and seldom used ACIDs. ACIDs not used for more than 59 days are suspended in the TOP SECRET security file. This complies with the requirements of both the National Institute of Standards and Technology and the General Accounting

Office Federal Information Systems Controls Audit Manual.
Contractor ACIDs are established for no more than one year, and annual renewal is required thereafter. Additionally, a file is matched periodically against the payroll system to identify and deactivate ACIDs for employees who have left the Agency.

Following are our comments on specific recommendations.

Recommendation 1

Review employee job functions annually and access privileges to minimize the number of security control ACIDs and special privilege ACIDs in the TOP SECRET environment.

Comment

We agree with the intent of the recommendation. Established Agency policy requires review of employee job functions and access privileges within the mainframe environment, as well as modification of security profiles as appropriate. These reviews are ongoing, with their frequencies depending upon changing systems functionality, and involve both security and operational personnel. Agency security officers are required to submit to the SSAISSO maintenance requests modifying TOP SECRET profile access when transactions or groups of transactions are no longer necessary. SSA components have been required to perform comprehensive evaluations of TOP SECRET access profiles, and, as appropriate, such evaluations have led to consolidation and/or elimination of profiles and systems access. Both ongoing and periodic evaluations are driven by the concept of least privilege access.

To reinforce these review requirements, by the end of fiscal year 2000 a memorandum will be issued to remind Agency components of the need to continue the practice of reviewing job functions and systems access.

Recommendations 2 and 5

Remove inactive ACIDs from the TOP SECRET security file.

Establish policy and procedures to automatically remove inactive ACIDs.

Comment

We agree with the intent of these recommendations; however the specifically recommended approach is not feasible. Instead of removing inactive ACIDs from the TOP SECRET security file, we will deactivate them and keep them on the file. This approach allows full functionality of the software utility we use to execute audits of the security file. Without record of these ACIDs, the utility would fail.

Recommendation 3

Establish a procedure to monitor and document periodic reviews of access violation reports to detect access compromises in a timely manner.

Comment

We agree and have implemented procedures for weekly reviews and documentation of access violations.

Recommendation 4

Establish a procedure to perform continuous reviews of Terminal Sharing Options users access privileges in accordance with the least privilege concept.

Comment

We agree and are evaluating options for ensuring such continuous reviews. We expect to select the appropriate option by the end of December 2000.

Other Matters

The first footnote in the OIG report (page 5) indicates that CONSOLE privileges allow individuals to execute tasks or change security control options. CONSOLE privileges actually only allow modification of security control options.

The second footnote (page 5) states that new password change privileges allow individuals to customize password security rules. As noted in the opening section above, only 17 users have full CONSOLE authority. Therefore, other users cannot change the rules.

OIG Contacts and Staff Acknowledgements

OIG Contacts

Pat Kennedy, Audit Manager, Systems Audit Division
(410) 965-9724

Acknowledgments

In addition to those named above:

Mary Ellen Fleischman, Program Analyst

Greg Hungerman, Program Analyst

Kimberly Beauchamp, Writer-Editor, Policy, Planning and Technical Services
Division

For additional copies of this report, please contact the Office of Inspector General's Public Affairs Specialist at (410) 966-5998. Refer to Common Identification Number A-14-99-11001.

DISTRIBUTION SCHEDULE

	<u>No. of Copies</u>
Commissioner of Social Security	1
Management Analysis and Audit Program Support Staff, OFAM	10
Deputy Commissioner for Office of Systems	1
Deputy Commissioner for Finance, Assessment and Management	1
Inspector General	1
Assistant Inspector General for Office of Investigations	1
Assistant Inspector General for Office Executive Operations	3
Assistant Inspector General for Management Services	1
Assistant Inspector General for Audit	1
Deputy Assistant Inspector General for Audit	1
Director, Systems Audit Division	1
Director, Financial Management and Performance Monitoring Audit Division	1
Director, Operational Audit Division	1
Director, Disability Program Audit Division	1
Director, Program Benefits Audit Division	1
Director, General Management Audit Division	1
Issue Area Team Leaders	16
Total	<u>43</u>

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.