Office of the Inspector General

September 24, 1999

John R. Dyer
Principal Deputy Commissioner
of Social Security

Acting Inspector General

Employee Access to Title XVI Computer Applications and Data (A-13-98-12009)

Attached is a copy of the subject final report. The objective of our audit was to determine whether, based on job duties, employees had appropriate levels of access to Supplemental Security Income computer applications and data.

You may wish to comment on any further action taken or contemplated on our recommendations. If you choose to offer comments, please provide them within the next 60 days. If you wish to discuss the final report, please call me, or have your staff contact Daniel R. Devlin, Acting Assistant Inspector General for Audit, at (410) 965-9700.

James G. Huse, Jr.

Attachment

OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

EMPLOYEE ACCESS TO TITLE XVI COMPUTER APPLICATIONS AND DATA

September 1999 **A-13-98-12009**

AUDIT REPORT

EXECUTIVE SUMMARY

OBJECTIVE

The objective of this audit was to determine whether, based on job duties, employees have appropriate levels of access to Supplemental Security Income (SSI) computer applications and data.

BACKGROUND

There are concerns that information protection-related weaknesses subject sensitive Social Security Administration (SSA) information to potential unauthorized access, modification, and/or disclosure by employees. The U.S. General Accounting Office (GAO) reported that the SSI program has been affected by internal control weaknesses, complex policy issues, and insufficient management attention. For these reasons, GAO identified the SSI program as "high-risk" in February 1997. Additionally, PricewaterhouseCoopers (PWC) (formerly Price Waterhouse), SSA's financial statement audit contractor, recommended that the lack of controls in protecting information be reported as a material weakness in SSA's annual Federal Managers' Financial Integrity Act report for Fiscal Year 1997.

The SSI program, authorized by title XVI of the Social Security Act, is a needs-based program administered by SSA. The primary automated system for processing SSI claims is the Modernized Supplemental Security Income Claims System (MSSICS). MSSICS is a mainframe-based, on-line, interactive claims system. The system allows for the establishment and processing of SSI claims by accumulating data, such as identification information, the disability determination decision, living arrangements, financial resources, income, and potential eligibility for other benefits. SSA controls employee access to MSSICS and other production mainframe computer resources (i.e., data files, application and system software programs, and computer-related facilities and equipment) through the use of Computer Associates-TOP SECRET, or simply TOP SECRET.

The Office of Management and Budget (OMB) requires that agencies incorporate security controls into sensitive financial management systems. One basis for assigning proper access is "least privilege" which is defined as the practice of restricting a user's access to the minimum amount necessary to perform job duties or responsibilities. One of TOP SECRET's primary mechanisms for controlling user access is through the use

of profiles.[1] Profiles are sets of transaction identifiers (ID) for groups of users and are generally defined and assigned according to job position. These transaction IDs permit access to specific MSSICS computer screens. SSA uses two types of profiles: standardized and nonstandardized. Standardized profiles are defined as profiles that remain fixed within the Agency. These profiles are most applicable to operational positions that are standardized across field locations throughout SSA. Nonstandardized profiles are generally developed within a component for a particular person, position, or team and are not standard across field locations or components such as SSA's Office of Systems personnel.

We reviewed all 281 standardized MSSICS profiles and identified 62 that provided access to at least 1 of 8 transaction IDs that are gateway screens for sensitive data entry or updating functions. Of the 62 profiles, we identified 22 profiles with access privileges that did not appear excessive using job descriptions as a guide. The remaining 40 profiles were assigned to 30,450 personal identification numbers (PIN) that potentially had excessive access. We discussed with security personnel how these profiles are developed, assigned, and reviewed. SSA could not readily determine the number of nonstandardized profiles because it would have required a massive manual effort to produce.

RESULTS OF REVIEW

STANDARDIZED TOP SECRET PROFILES PROVIDED EXCESSIVE ACCESS TO MSSICS

Of the 62 standardized TOP SECRET profiles we reviewed, 19 (31 percent) provided MSSICS update capabilities in excess of those needed by SSA personnel to perform job duties. These 19 profiles control access for 25,330 unique and nonunique PINs.[2] One of these profiles was assigned to over 7,500 unique PINs. As a result, employees using these 25,330 PINs could inadvertently or intentionally change information on SSI files or send inaccurate data to SSI records. This condition existed for several reasons: (1) MSSICS software was not designed so that transaction IDs could be assigned to profiles to achieve adequate segregation of high- and low-risk data entry fields on the computer screens; (2) security personnel did not change profiles as job positions evolved; (3) security personnel erroneously assigned improper access; and (4) SSA's Systems Security Officer (SSASSO) staff did not adequately review proposed profiles and did not periodically review profiles to ensure that they remained appropriate. We did not determine whether any excessive transactions were executed as a result of excessive access because it was not practical for us to do so. Even without testing, we

[1] TOP SECRET's two other types of mechanisms for controlling access (data sets and transaction identifiers assigned directly to individual users rather than being assigned to profiles) were not covered under the scope of this review.

[2] These PINs can be assigned multiple profiles. Because we counted profiles, PINs can be counted more than once. PINs that are assigned more than one profile are considered nonunique, while PINs that are assigned only one profile are considered unique. (See Exhibit 1 on page 3 for illustration.)

believe the significant number of PINs (over 25,000) with excessive access results in increased exposure to fraud, waste, and abuse in the SSI program.

NONSTANDARDIZED TOP SECRET PROFILES FOR MSSICS WERE NOT ADEQUATELY CONTROLLED OR MANAGED

SSA did not adequately control or manage employees' access privileges through nonstandardized MSSICS profiles. Nonstandardized profiles are created and controlled within a component and are not subject to review outside that component by SSASSO. As a result, SSA cannot determine, without a massive manual effort, the number of employees, including analysts and programmers, who may have inappropriate access to input or modify sensitive SSI data. We believe SSA's ineffective control and management of its employees' access privileges continues because SSA has implemented the profiles in such a way that the readily available reporting and control mechanisms in TOP SECRET cannot be effectively utilized without additional programming to monitor and review the access.

CONCLUSIONS AND RECOMMENDATIONS

SSA needs to strengthen security access controls for the 25,330 unique and nonunique PINs having excessive access. Excessive access could result in loss of data, loss of funds, and the unauthorized release of personal information. This vulnerability increases SSA's exposure to fraud in the SSI program. To establish proper security controls and effectively implement the policy of least privilege, SSA needs to restrict authorized employee access. SSA also needs to improve security officers' monitoring and oversight of the granting of access throughout SSA.

FINDING: STANDARDIZED TOP SECRET PROFILES PROVIDE EXCESSIVE ACCESS TO MSSICS

We recommend that SSA:

- Remove excessive or inappropriate transaction IDs from those profiles identified as having excessive access (see Appendix A).

- Examine the activity in the audit trail files of all PINs assigned to the profiles identified in Appendix A to determine whether excessive transactions were performed which may indicate fraud and refer any violations to the Office of the Inspector General (OIG).

- Review all other MSSICS TOP SECRET profiles and remove those transaction IDs that permit inappropriate or excessive access for the assigned duties and responsibilities.

- Modify MSSICS software to segregate access between high- and low-risk data entry fields.

- Provide improved training and guidance to security officers assigning and reviewing transaction IDs to standardized TOP SECRET profiles for which they are responsible. As part of this training, SSA should provide improved system flow charts and functional descriptions of new transaction IDs, particularly for major software releases when many new capabilities are added.

- Perform periodic post-implementation reviews of profiles by security staff for proper assignment of transaction IDs to profiles based on the concept of least privilege.

FINDING: NONSTANDARDIZED TOP SECRET PROFILES FOR MSSICS ARE NOT ADEQUATELY CONTROLLED OR MANAGED

We recommend that SSA:

- Require that SSASSO staff review and approve all access to production data.

- Accelerate efforts to develop standardized profiles for all positions requiring access and increase security officer review and approval of the granting and deletion of nonstandardized profiles.

AGENCY COMMENTS

With the exception of the following comments, SSA concurred with our recommendations.

- In the first recommendation, SSA did not agree that access for the Model District Office (MDO) Manager profile was excessive. Instead, the Agency contends that the MDO Manager profile requires access to high-risk transactions during implementation weekends when software is tested before it is released to the regions. To ensure that MDO Manager access is issued only for testing software applications, SSA plans to review this access for implementation weekends.

- In the second recommendation, SSA recognized the need to detect fraud but rejected our recommendation on the basis of cost. SSA believes other processes are already in place to adequately detect fraud.

- SSA took exception to the sixth recommendation because it believes line management is responsible for post-implementation and that security personnel are accountable for administering access control policies, standards, and procedures approved by the SSASSO and/or senior management.
- Similarly, SSA did not agree with the seventh recommendation for SSASSO staff to review and approve all access to production data. While SSA agrees there is a need to review and approve standardized and nonstandardized profiles, the Agency

does not believe this function is SSASSO's responsibility. Again, SSA contends that this review and approval is the best performed by line management. SSA believes that its planned approach for developing standardized profiles will provide more effective controls over access to production data.

SSA also provided two technical comments. First, the Agency is concerned that our definition of standardized profiles could imply that these profiles remain fixed. Second, SSA had concerns that our use of the term "nonunique" to describe PINs assigned to more that one profile could give the impression that some users are assigned more than one PIN. The full text of SSA's comments is included in Appendix B.

OIG RESPONSE

We continue to support our recommendations. Based on SSA's comments, we have the following responses.

- With regard to the first recommendation, we still believe the excess access for the MDO Manager profile should be removed. First, MDO Managers are not frequently involved in implementation weekends. At a minimum, SSA should limit MDO Manager access by using separate profiles that are only available to MDO Managers during implementation weekends. Second, SSA's plan to audit high-risk transactions during implementation weekends does not acknowledge that high-risk transactions may be occurring at times other than on implementation weekends.

- While we acknowledge there are costs associated with implementing the second recommendation, we contend that SSA must fully use the audit trail files that were created to detect fraud.

- For recommendations six and seven, we still believe the role of security personnel include: periodic reviews of profiles and responsibility for reviewing and approving access to production data. We acknowledge that the assignment of profiles to individual users is the responsibility of line management. However, both recommendations refer to the assignment of transition ID's to profiles—a function that should be the responsibility of security personnel.

We considered SSA's technical comments while drafting our report. Even with the assistance of SSA staff, we were unable to come up with more appropriate terminology. We believe the inclusion of the technical comments in the report will minimize any of the reader's misconceptions.

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

INTRODUCTION 1

RESULTS OF REVIEW 6

STANDARDIZED TOP SECRET PROFILES PROVIDED EXCESSIVE ACCESS TO MSSICS 6

NONSTANDARDIZED TOP SECRET PROFILES FOR MSSICS WERE NOT ADEQUATELY CONTROLLED OR MANAGED 8

CONCLUSIONS AND RECOMMENDATIONS 10

APPENDICES
APPENDIX A - Top Secret Profiles Having Excessive Access
APPENDIX B - SSA Comments
APPENDIX C - Major Contributors to This Report
APPENDIX D - SSA Organizational Chart

INTRODUCTION

OBJECTIVE

The objective of this audit was to determine whether, based on job duties, employees had appropriate levels of access to the Supplemental Security Income (SSI) computer applications and data.

BACKGROUND

The Office of Management and Budget (OMB) Circular A-127, Financial Management Systems, requires that Federal agencies plan for and incorporate security controls into sensitive financial management systems. OMB Circular A-130, Management of Federal Information Resources, requires that agencies: (1) maintain and protect individuals identifiable information and proprietary information in a manner that precludes unwarranted intrusion upon personal privacy and violation of confidentiality; (2) ensure agency personnel are trained to safeguard information resources; (3) establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system; and (4) ensure that only authorized personnel have access to information systems. OMB Circular A-130 also requires that agencies incorporate personnel controls, such as separation of duties, least privilege, and individual accountability to ensure that adequate security is provided for an agency's major applications. Least privilege is defined as the practice of restricting a user's access to data files, processing capabilities, or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job. The Social Security Administration (SSA) has incorporated this principle as a standard in its Systems Security Handbook. In fact, the Handbook states ". . . controlling and limiting access is the *first line of defense* in assuring the security and integrity of Agency resources."

SSA's Systems Security Officer (SSASSO) staff, along with a network of regional and Central Office component security staff members, have overall responsibility for interpreting, developing, and implementing security policy. Security officers are responsible for developing, implementing, and managing the security program within their organizations, including administration of access controls. According to the Systems Security Handbook, SSASSO staff provides guidance and advises security officers in matters involving SSA's security program, establishes systems security policies and procedures, and administers the Computer Associates TOP SECRET (TOP SECRET) profile access authorization matrix.

Title XVI Program and Applications

The SSI program, authorized by title XVI of the Social Security Act, is a needs-based program administered by SSA. SSI provides a minimum level of income to people who are aged, blind, disabled, and/or who have limited income and resources. During Fiscal Year (FY) 1998, qualifying individuals could receive a maximum of $494 in Federal benefits per month plus medical assistance. Some States provide supplementary benefits that are paid by SSA, but SSA receives reimbursement from those States for the supplementary benefits it pays. In FY 1998, SSA paid out $30.5 billion in SSI and supplementary State benefits to more than 6.6 million recipients. SSI payments are not paid from the Social Security or Medicare trust funds, but from the general fund of the U.S. Department of the Treasury.

The primary automated system for processing SSI claims is the Modernized Supplemental Security Income Claims System (MSSICS). MSSICS is a mainframe-based, on-line, interactive claims system using screens allowing for the establishment and adjudication of SSI claims. MSSICS accumulates claimant data, such as identification information, the disability determination decision, living arrangements, financial resources, income, and potential eligibility for other benefits. SSA first implemented MSSICS in 1992, with the latest major release in May 1997 to add post-entitlement processing capabilities.

Access Control Software

SSA uses TOP SECRET, a commercial access control software package, to control employee access to MSSICS and other production mainframe computer resources. TOP SECRET protects computer resources by identifying authorized users and controlling their access capability.

To obtain access to SSA's systems through TOP SECRET, an employee first submits Form SSA-120, Application for Access to SSA Systems, to the designated local security officer. After the application is approved, it is forwarded to the appropriate regional or component security officer, who assigns a personal identification number (PIN) and initial password. The PIN is assigned as many profiles as the employee needs to perform his or her job duties.

One of TOP SECRET's primary mechanisms for controlling user access is the profile. Profiles contain sets of common access authorizations referred to as transaction identifications (ID) for groups of users. Access authorizations allow specific data entry transactions and query capabilities for each computer screen. SSA defines and assigns standardized profiles according to job position. SSA has developed more than 1,700 standardized profiles to control systems access for about 127,000 unique and nonunique PINs assigned to these profiles.

PINs may be assigned to more than one profile. A PIN is considered nonunique if it has more than one profile assigned. Therefore, nonunique PINs are counted more than once in summary totals. An illustration of unique versus nonunique PINs is shown in Exhibit 1.

Exhibit 1. Illustration of Unique Versus Nonunique PINs

Employee Name	*PIN*	*No. of Profiles Assigned*	*Unique/Nonunique*
Tom	*001*	*2*	*Nonunique*
Mary	*002*	*3*	*Nonunique*
Joe	*003*	*1*	*Unique*
Sue	*004*	*2*	*Nonunique*

SUMMARY PROFILE REPORT		
Profile	***PINs Assigned***	***No. of PINs***
Profile 1	001 002 004 etc.	3,000
Profile 2	001 003 etc.	2,000
Profile 3	002 etc.	1,000
Profile 19	002 004 etc.	5,000
Total PINs (All Profiles)		**127,000**

We have identified 281 of the standardized profiles assigned to 73,500 PINs providing access to the MSSICS application. Standardized profiles are defined as profiles that are reviewed, approved, and controlled by SSASSO. These profiles are most applicable to operational positions, such as benefit authorizers, which are standard throughout SSA's field locations. Nonstandardized profiles are generally defined as profiles that are developed within a component for a particular person, position, or team and are not standard across organizations such as SSA's Office of Systems (OS) personnel. SSA did not use standardized profiles in OS because of the diverse nature of duties for OS personnel. Nonstandardized profiles are not reviewed or approved by SSASSO, and may be custom-designed for one or more individuals.

MSSICS contains nearly 400 transaction IDs. Transaction IDs permit a user to access different computer screens, containing various data entry fields, for performing specific activities such as establishing a new claim, updating post-entitlement data, providing a path or "gateway" to other input screens, and/or performing data queries.

SCOPE AND METHODOLOGY

We obtained a listing and general description of the 396 MSSICS transaction IDs and found 8 of the transaction IDs were most critical for processing or updating information. We also obtained 281 standardized MSSICS profiles and identified 62 that provided access to at least 1 of the 8 transaction IDs we identified as gateway screens. These 62 profiles allow employees to input and update data in MSSICS.

Exhibit 2: Critical Transaction IDs

	Transaction ID	Description	Purpose of Transaction ID
1.	ZA05	SSI Claims Application, Establish, Full/Deferred	Collects application and eligibility data.
2.	ZA15	Client Identification, Full/Deferred	Records personal identification data about the claimant.
3.	ZJ30	Decision Input, Update	Records adjudicative decisions.
4.	ZJ95	Build Supplemental Security Record (SSR)	Begins the process that builds the SSR.
5.	ZJP3	Decision Input, Close Post-Entitlement Events	Records adjudicative decisions.
6.	ZM11	Person Screen Status (Establish, Update)	Displays all available screens in the claimant's path and allows selection of those screens for updating.
7.	ZM42	Post-Entitlement Menu	Allows entry to post-entitlement screens.
8.	ZS97	Build Transaction SSR Confirmation	Instructs MSSICS to send completed data to the SSR.

Of the 62 profiles identified as having input and update access to MSSICS, we identified 22 profiles with access privileges that did not appear excessive using job position descriptions as a guide. For the remaining 40 profiles, we obtained a more in-depth understanding of users' job duties actually performed through discussions with personnel within the Office of Operations and the Office of Finance, Assessment and Management about the position descriptions and training requirements.

The 40 profiles control access for approximately 30,450 unique and nonunique PINs among the following 4 SSA offices or components:

- Office of Quality Assistance and Performance Assessment (OQA),
- Office of Automation Support (OAS),[3]
- Office of Central Operations, and
- SSASSO's office.

We also discussed with the Office of Operations the inadequacy of the MSSICS system to permit the segregation of high- and low-risk data entry fields. In addition, we

[3] OAS administers profiles for SSA's field offices, teleservice centers, area directors' offices, regional offices, and Headquarters offices.

reviewed a typical nonstandardized profile used by SSA's Office of Systems Requirements (OSR). We also reviewed SSA's Modernized Systems Operations Manual and the Systems Security Handbook to determine pertinent operating and security policies and procedures. We discussed with security personnel in each of the four offices mentioned above how profiles are developed using the system documentation of transaction IDs and how they are assigned and reviewed.

We did not determine the extent to which individuals were assigned multiple profiles; whether assignment of multiple profiles provided too broad an access; or whether job positions had excessive functions. These issues are subject to an ongoing review by SSA's PWC. We did not determine whether individuals had executed any improper transactions as a result of excessive access because it was not practical for us to do so.

We also planned to determine the number of employees in OS, including systems analysts and programmers, who have improper access to input or modify MSSICS data. However, despite our requests, SSA did not provide a listing of nonstandardized profiles with access to MSSICS data for our review, including the number of PINs assigned to these profiles, because of resource restraints. Although SSA did not provide a list of nonstandardized profiles, it did provide an example of a typical nonstandardized profile for our review. In addition, we did not review the access of those employees who have access assigned through datasets or transaction IDs directly.

We conducted the audit from January through May 1998 at SSA Headquarters in Baltimore, Maryland. The audit was performed in accordance with generally accepted government auditing standards.

RESULTS OF REVIEW

We found that employee access to title XVI computer applications and data using standardized profiles was excessive, and the use of nonstandardized profiles is not adequately controlled.

STANDARDIZED TOP SECRET PROFILES PROVIDED EXCESSIVE ACCESS TO MSSICS

We reviewed 62 standardized TOP SECRET profiles identified as having input and update access to MSSICS and found 19 (31 percent) provided employees with input and update capabilities in excess of those needed to perform their job duties. One of these profiles controlled access for over 7,500 unique PINs. In total, the 19 profiles controlled access for 25,330 unique and nonunique PINs. Specifically, 7 of the 19 standardized TOP SECRET profiles were assigned to approximately 18,800 PINs in SSA field offices and program service centers. These seven profiles provided excessive access to update functions that the employees assigned to these profiles were neither trained nor authorized to process. The remaining 12 of the 19 standardized TOP SECRET profiles were assigned to over 6,500 PINs throughout several SSA components, including SSASSO staff. In these 12 instances, excessive access exposed sensitive SSA data to unauthorized access, modification, and disclosure by individuals who had no job-related need for this access (see Appendix A for details). This data involves information related to Social Security numbers, disabilities, and title XVI benefits. As a result, employees could inadvertently or intentionally change data and files affecting the amount of SSI benefits and recipient. Even though we did not determine whether any fraudulent activities occurred, the repercussions of such actions could be far reaching because of the large number of PINs assigned to these profiles.

OMB Circular A-130 requires that agencies incorporate personnel controls, including least privilege, to ensure that adequate security is provided for an agency's major applications. Least privilege is the practice of restricting a user's access to data files, processing capabilities, or type of access to the minimum necessary to perform job duties. SSA's Rules of Behavior for Users and Managers in SSA's Systems Security Handbook also specifies systems access is to be restricted to that needed to perform assigned duties.

SSA employees were given authority to access systems in excess of that needed to perform their job duties for four reasons: (1) MSSICS software was not designed so that transaction IDs could be assigned to profiles to achieve adequate segregation of high- and low-risk data entry fields on the computer screens; (2) security personnel did

not change profiles as job positions evolved; (3) security personnel incorrectly assigned improper access; and (4) SSASSO did not adequately review proposed profiles and did not periodically review profiles to ensure they remain appropriate.

MSSICS Software Limitations MSSICS software is not designed to allow for proper segregation of low- and high-risk data entry fields on the screens when assigning transaction IDs to profiles. SSA considers high-risk data entry fields as those that allow the user to establish a new claim or process significant post-entitlement actions resulting in a redetermination of benefits. Low-risk data entry fields are those that do not affect the amount of benefit payment or result in a redetermination review, such as direct deposit data and a change of address not resulting in a change in living arrangements.

Some positions need access to MSSICS screens containing more data entry fields than are needed to perform their job duties. Operations supervisors, field representatives, generalist claims representatives, and title XVI claims representatives are authorized to update high-risk data entry fields and are the only positions authorized to establish new claims and fully adjudicate post-entitlement actions. However, standardized profiles for title II claims representatives, service representatives, telephone service representatives, inquiry and expediting specialists, SPIKES, and claims recovery technical assistants include access to screens that allow these unauthorized staff to update high-risk data entry fields. Access to the high-risk data fields by these employees is unavoidable because the screens they use contain both the necessary low-risk fields and the unnecessary high-risk fields. MSSICS software cannot suppress the high-risk data fields so that these employees are limited in their access to only the needed low-risk data fields. During our audit, we found that OAS was already aware of this software limitation and had submitted a request to OS to correct the problem. However, according to OAS, OS had not been able to respond to its request because of higher priority projects.

Profiles Were Not Changed as Job Positions Evolved Security personnel in OAS did not change standardized profiles as job duties for certain positions evolved because there was no specific requirement for security personnel to review and modify profiles when job duties changed. It was not clear why security personnel did not adhere to SSA's Systems Security Handbook policy to ensure that excessive access was not granted. Development clerks and data entry operators have access to all of the transaction IDs needed to establish an initial claim and enter post-entitlement actions—transactions typically reserved for claims representatives and field representatives. According to OAS management, the necessity for those positions to retain such extensive access was significantly reduced or completely eliminated with the implementation of SSA's Intelligent Workstation project. Over time, field representatives have become able to carry out their own data entry tasks more quickly and efficiently using remote workstations rather than relying on development clerks and data entry operators.

Improper Access Assigned Security personnel incorrectly assigned improper access because of lack of guidance or inadequate understanding of the capabilities of the transaction IDs involved. In OQA and SSASSO, security personnel were inadvertently or unknowingly assigned transaction IDs providing them the capability to update or modify certain data in the MSSICS pending file when query only access was all that was needed. After we discussed this with component security personnel during our audit, both OQA and SSASSO agreed that the standardized profiles provided excessive access, and they have initiated appropriate profile changes. OAS has also initiated some of the profile changes we recommended during our audit. We believe these types of mistakes occurred because OSR did not provide sufficient system flowcharts, screen paths, and functional descriptions of transaction IDs to assist component security officers to properly construct standardized profiles for each respective component. In addition, limited training was provided on the effect the new system features have on access rights that may require modifications to existing profiles. For example, for the last major release of MSSICS software, 78 new screens were added. While OSR provided facsimiles of the new screens and a listing of new transaction IDs to security officers at the security kickoff meeting, they did not provide adequate screen and transaction ID descriptions and pathing flowcharts. Descriptive guidance was provided for only 16 of the 78 new transaction IDs. Additionally, security officers had only a short time to develop new profiles and submit them to SSASSO for review.

Inadequate Review of Profiles SSASSO staff is responsible for reviewing and approving all new or modified standardized profiles before they are implemented and validating the access granted by the profiles. During its initial profile reviews, SSASSO staff did not detect or prevent the erroneous transaction IDs from being assigned. We could not determine why security personnel did not adhere to the Systems Security Handbook policy requiring least privilege. While not specifically required, security personnel did not perform periodic reviews to ensure profiles contained appropriate transaction IDs.

SSA had not identified all employees with these excessive accesses nor determined whether any of them had inappropriately made transactions. Without examining audit trail files to determine whether individuals had used their excessive access to execute any improper transactions, it is impossible to determine whether fraud or abuse has occurred.

NONSTANDARDIZED TOP SECRET PROFILES FOR MSSICS WERE NOT ADEQUATELY CONTROLLED OR MANAGED

SSA did not adequately control or manage nonstandardized profiles for employees in OS. Access for these employees is neither assigned through the use of standardized profiles nor reviewed or approved by SSASSO. Security personnel in OS create and implement these profiles independent of SSASSO oversight. We could not determine why SSASSO did not review or approve these profiles to ensure excessive access was

not granted as required by the Systems Security Handbook. As a result, there was no oversight to ensure sensitive SSI information was protected from unauthorized access, modification, and disclosure. Excessive access allows employees to inadvertently or intentionally update information on the MSSICS pending file and the SSR. Unauthorized changes or modifications to these SSI records could result in a change in a claimant's eligibility and benefit amount.

Although SSA could not readily provide a listing of nonstandardized profiles for our review, it did provide an example of a typical nonstandardized profile for an undetermined number of systems analysts in OSR. We found these analysts could input or change data associated with two of the eight sensitive transaction IDs, as described in the Scope and Methodology section of this report.

As stated earlier, OMB Circular A-130 requires that agencies incorporate personnel controls to ensure that adequate security is provided for an agency's major applications. According to SSA's Systems Security Handbook, security officers are responsible for developing, implementing, and managing security within their offices. Their responsibilities include administering, monitoring, and assessing compliance of access controls.

We believe SSA's ineffective control and management of its employees' access privileges continues because SSA has implemented the profiles in such a way that the readily available reporting and control mechanisms in TOP SECRET cannot be effectively utilized without additional programming to monitor and review the access. During our audit, one security officer stated that nonstandardized profiles were extremely difficult to administer because each employee's access had to be administered individually. For this reason, we support SSA's initiative to move toward eliminating nonstandardized profiles and replacing them with standardized profiles.

We acknowledge that SSA has taken some preliminary steps toward classifying and developing standardized profiles for employees in OS, which make up the majority of nonstandardized users. OS established a workgroup in November 1997 to address these access issues. As of April 1999, the workgroup had made some progress toward developing and implementing standardized profiles for users having access to on-line production systems. SSA anticipates Phase I of this project will be completed by December 31, 1999. However, as of the date of this audit, only 12 of an estimated 125 profiles had been completed, and 35 others were under development. SSA needs to make this project a higher priority in order to ensure its successful and timely completion.

CONCLUSIONS AND RECOMMENDATIONS

SSA needs to strengthen security access controls for the 25,330 unique and nonunique PINs that have excessive access. Excessive access could result in loss of data, loss of funds, and the unauthorized release of personal information. This vulnerability increases SSA's exposure to fraud in the SSI program. In order to establish proper security controls and effectively implement the policy of least privilege, SSA needs to restrict authorized employee access to that needed to perform assigned duties. SSA also needs to improve security officers' monitoring and oversight of the granting of access throughout SSA.

FINDING 1: STANDARDIZED TOP SECRET PROFILES PROVIDED EXCESSIVE ACCESS TO MSSICS

We recommend that SSA:

1. Remove excessive or inappropriate transaction IDs from those profiles identified as having excessive access (see Appendix A).

2. Examine the activity in the audit trail files of all PINs assigned to the profiles identified in the Appendix to determine whether excessive transactions were performed to commit fraud and refer any violations to the OIG.

3. Review all other MSSICS TOP SECRET profiles and remove those transaction IDs that permit inappropriate or excessive access for the assigned duties and responsibilities.

4. Modify MSSICS software to segregate access between high- and low-risk data entry fields.

5. Provide improved training and guidance to security officers assigning and reviewing transaction IDs to standardized TOP SECRET profiles for which they are responsible. As part of this training, SSA should provide improved system flow charts and functional descriptions of new transaction IDs, particularly for major software releases when many new capabilities are added.

6. Perform periodic post-implementation reviews of profiles by security staff for proper assignment of transaction IDs to profiles based on the concept of least privilege.

FINDING 2: NONSTANDARDIZED TOP SECRET PROFILES FOR MSSICS ARE NOT ADEQUATELY CONTROLLED OR MANAGED

We recommend that SSA:

7. Require that SSASSO staff review and approve all access to production data.

8. Accelerate its efforts to develop standardized profiles for all positions requiring access and increase security officer review and approval of the granting and deletion of nonstandardized profiles.

AGENCY COMMENTS

With the exception of the following comments, SSA concurred with our recommendations. The full text of SSA's comments is included in Appendix B.

- In the first recommendation, SSA did not agree that access for the MDO Manager profile was excessive. Instead, the Agency contends that the MDO Manager profile requires access to high-risk transactions during implementation weekends when software is tested before it is released to the regions. To ensure that MDO Manager access is issued only for testing software applications, SSA plans to review this access for implementation weekends.

- In the second recommendation, SSA recognized the need to detect fraud but rejected our recommendation on the basis of cost. SSA believes other processes are already in place to adequately detect fraud.

- SSA took exception to the sixth recommendation because it believes line management is responsible for post-implementation and that security personnel are accountable for administering access control policies, standards, and procedures approved by the SSASSO and/or senior management.

- Similarly, SSA did not agree with the seventh recommendation for SSASSO staff to review and approve all access to production data. While SSA agrees there is a need to review and approve standardized and nonstandardized profiles, the Agency does not believe this function is SSASSO's responsibility. Again, SSA contends that this review and approval is the best performed by line management. SSA believes that its planned approach for developing standardized profiles will provide more effective controls over access to production data.

SSA also provided two technical comments. First, the Agency is concerned that our definition of standardized profiles could imply that these profiles remain fixed. Second,

SSA had concerns that our use of the term “nonunique” to describe PINs assigned to more that one profile could give the impression that some users are assigned more than one PIN.

OIG RESPONSE

We continue to support our recommendations. Based on SSA’s comments, we have the following responses.

- With regard to the first recommendation, we still believe the excess access for the MDO Manager profile should be removed. First, MDO Managers are not frequently involved in implementation weekends. At a minimum, SSA should limit MDO Manager access by using separate profiles that are only available to MDO Managers during implementation weekends. Second, SSA’s plan to audit high-risk transactions during implementation weekends does not acknowledge that high-risk transactions may be occurring at times other than on implementation weekends.

- While we acknowledge there are costs associated with implementing the second recommendation, we contend that SSA must fully use the audit trail files that were created to detect fraud.

- For recommendations six and seven, we still believe the role of security personnel include: periodic reviews of profiles and responsibility for reviewing and approving access to production data. We acknowledge that the assignment of profiles to individual users is the responsibility of line management. However, both recommendations refer to the assignment of transition ID’s to profiles—a function that should be the responsibility of security personnel.

We considered SSA’s technical comments while drafting our report. Even with the assistance of SSA staff, we were unable to come up with more appropriate terminology. We believe the inclusion of the technical comments in the report will minimize any of the reader’s misconceptions.

APPENDICES

TOP SECRET PROFILES HAVING EXCESSIVE ACCESS

The Social Security Administration's 12 TOP SECRET profiles identified by the Office of the Inspector General as having inappropriate or excessive access.

	Profile	No. of PINs Assigned	Component	Position	High-Risk Transaction IDs Not Needed
1.	POI118P	1,210	OQA	General	ZA15, ZJ30, ZJP3
2.	POI166P	21	OQA	Regional/Local Security Officer	ZA15, ZJ30, ZJP3
3.	POI167P	20	OQA	Alternate Regional Security Officer	ZA15, ZJ30, ZJP3
4.	POI168P	29	OQA	Local Security Officer	ZA15, ZJ30, ZJP3
5.	POI169P	18	OQA	Alternate Local Security Officer	ZA15, ZJ30, ZJP3
6.	POI348P	9	OQA	National Disability Determination Service System Disability Insurance Quality Reviewer	ZA15, ZJ30, ZJP3
7.	PRO765P	10	OAS	Model District Office Manager	ZA05, ZA15, ZJ30, ZJ95, ZS97
8.	PRX015P	39	OAS	Operations Officer	ZJ95, ZM11, ZS97
9.	PRX016P	43	OAS	Staff Assistant	ZJ95, ZM11, ZS97
10.	PRX026P	4,252	OAS	Development Clerk	ZA05, ZA15
11.	PRX287P	913	OAS	Data Entry Operator	ZA05, ZA15
12.	PSS843P	3	SSASSO	Management Analyst	ZJ30
TOTAL PINs		**6,567**			

APPENDIX B

SSA COMMENTS

MAJOR CONTRIBUTORS TO THIS REPORT

Office of the Inspector General

Donald G. Franklin, Director, Systems Audits

Albert J. Darago, Audit Manager

Randy J. Townsley, Auditor-in-Charge

Anita M. McMillan, Senior Systems Auditor

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-13-98-12009.

APPENDIX D

SSA ORGANIZATIONAL CHART