Office of the Inspector General

November 30, 1998

Kenneth S. Apfel
Commissioner of Social Security

Acting Inspector General

Software Development and Maintenance Controls at the Social Security Administration

The attached final report presents the results of our review of software development and maintenance controls at the Social Security Administration (SSA) (A-13-96-11000). The objective of our review was to assess controls over application software development and maintenance at SSA.

You may wish to comment on any further action taken or contemplated. 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 Pamela J. Gardiner, Assistant Inspector General for Audit, at (410) 965-9700.

James G. Huse, Jr.

Attachment

OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

SOFTWARE DEVELOPMENT AND MAINTENANCE CONTROLS AT THE SOCIAL SECURITY ADMINISTRATION

November 1998 A-13-96-11000

AUDIT REPORT

EXECUTIVE SUMMARY

OBJECTIVE

The objective of this audit was to assess controls over application software development and maintenance at the Social Security Administration (SSA).

BACKGROUND

The Office of Management and Budget (OMB) Circular A-130, *Security of Automated Information Resources*, requires that a program be developed ensuring all information that is collected, processed, transmitted, stored, or disseminated in general support systems and major applications is adequately safeguarded. Also, the Privacy Act of 1974 requires that each agency maintaining a system of records have administrative, technical, and physical safeguards ensuring records are secure and kept confidential and protecting the records from any security or integrity hazard. To comply with these requirements, it is important to have a clearly defined approach to software development and maintenance. In 1985, SSA established the Software Engineering Technology (SET) manual defining the processes by which all systems are developed and maintained. It was also intended to document the standards, procedures, guidelines, and automated tools which are to be used in the software development and maintenance process. The latest revision to SET was in May 1994.[1] We initiated this audit to ensure that SSA is meeting these requirements.

Annually, SSA processes about 240 million earnings records, pays monthly benefits to over 50 million individuals, and issues new or replacement Social Security cards to about 16 million people. To accomplish this vital mission, SSA maintains an automated system that consists of four basic programmatic business functions: (1) enumeration; (2) earnings; (3) Retirement, Survivors and Disability Insurance claims and post-entitlement processing; and (4) Supplemental Security Insurance claims and post-eligibility processing. Each of these functions involves hundreds of software programs that are required to be developed according to SET. These programs are continuously being modified due to legislative changes and the initiatives set forth by the Commissioner of Social Security. Additionally, SSA is undertaking several major modernization projects to more efficiently serve the public, which includes distributing selected business functions between Headquarters and SSA's field components.

Field work was performed at SSA Headquarters in Baltimore, Maryland between

[1] There is also a 1997 draft version of SET that has not been implemented.

January and October 1997. We reviewed four software projects that were completed during 1996 for compliance with key SET requirements. Two were newly developed software and two were software maintenance releases for cyclical updates. This review focused primarily on the planning through the evaluation stages of SSA's systems development life-cycle (SDLC). The later phases of the SDLC were covered under a separate review.

RESULTS OF REVIEW

SSA's staff working on the four projects reviewed either did not follow SET procedures or substituted their own methods for documenting and controlling projects. We believe this occurred because SET is difficult to use, especially in today's dynamic systems environment. In addition, SET does not differentiate between mandatory standards and discretionary guidelines. Also, SSA is focused on piloting future methodologies and is no longer enforcing current standards. Specific findings were:

- authorizations that were required at key points in the SDLC were not always clearly documented;
- documentation was not kept in a central repository;
- critical problems that were identified during validation were not always resolved or analyzed for their effect; and
- quality assurance reviews were no longer being performed.

In its audit of SSA's Fiscal Year (FY) 1997 financial statements, PricewaterhouseCoopers[2] reported that SSA needs to improve its software application development, as well as change control policies and procedures, and consider this condition to be an internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA) of 1982. Our findings corroborate the concerns of PricewaterhouseCoopers. Weaknesses in the software development and maintenance process increase the risk that unauthorized or untested changes could be introduced into the production environment which would reduce the reliability of information being processed.

[2] Formerly known as Price Waterhouse.

CONCLUSIONS AND RECOMMENDATIONS

SSA needs to establish an organizational commitment toward greater consistency and discipline in its software development and maintenance process. We recommend that SSA:

- Enforce the requirements for authorizations and documentation at key points in the SDLC.

- Establish procedures in SET for maintaining critical documents in a central repository.

- Enforce the requirement that high priority problems discovered during validation be resolved before the software is released to production.

- Reinstate quality assurance reviews prescribed in SET.

SSA agreed with our recommendations. Currently SSA is implementing pilot projects relating to our first two recommendations. In response to our third recommendation, SSA stated that when possible, it will remove changes where problems have occurred and implement the changes in a later release. Finally, SSA stated that it plans to reinstate quality assurance reviews and is piloting integrated quality assurance reviews within the framework of the capability maturity model (CMM). Appendix A includes a copy of the complete text of SSA's comments.

TABLE OF CONTENTS

Page

APPENDICES

INTRODUCTION

OBJECTIVE

The objective of this audit was to assess controls over application software development and maintenance at SSA.

BACKGROUND

OMB Circular A-130, requires that a program be developed ensuring all information that is collected, processed, transmitted, stored, or disseminated in general support systems and major applications is adequately safeguarded. Also, the Privacy Act of 1974 requires that each agency maintaining a system of records have administrative, technical, and physical safeguards ensuring security and confidentiality of records and protecting those records from any anticipated security or integrity hazard. To comply with these requirements, it is important to have a clearly defined approach to software development and maintenance. SSA relies on SET standards and procedures to achieve the desired security and integrity within SSA systems.

Annually, SSA processes about 240 million earnings records, pays monthly benefits to over 50 million individuals, and issues new or replacement Social Security cards to about 16 million people. To accomplish this, SSA maintains an automated system that consists of four basic programmatic business functions: (1) enumeration; (2) earnings; (3) Retirement, Survivors and Disability claims and post-entitlement processing; and (4) Supplemental Security Insurance claims and post-eligibility processing. Each of these functions involves hundreds of software programs that are continuously being modified due to legislative changes and the Commissioner's initiatives. Also, SSA is undertaking several major modernization projects to better serve the public.

SSA's Dynamic Systems Environment

SSA is ending its reliance on centralized mainframe computers for programmatic applications. Instead, SSA is developing field-based computing systems to operate in cooperation with each other. Therefore, in the future, selected business functions will be distributed between Headquarters and SSA's field components for processing. This change presents a challenge. Applications will be more complex; thereby, increasing the need for new, more advanced skills. The staff that is developing, using, and maintaining the new applications will likely experience a cultural change. A well-defined, disciplined development and maintenance process will aid in supporting the staff in this environment. Equally important, this process will contribute significantly to the integrity and maintainability of the new applications.

SSA's Software Engineering Technology

In 1985, SSA developed a systems engineering environment management plan. Included in this plan was the SET manual. SET was developed to define the processes by which all systems are developed and maintained within SSA. By providing a framework of standards, procedures, and tools, SET is intended to:

- ensure the usability of software,
- maximize error detection in the early stages of development,
- improve software maintainability, and
- improve responsiveness to user requirements.

SSA has a new initiative to improve its software process. SSA's software process improvement program is following the capability maturity model that was recommended by the Software Engineering Institute at Carnegie Mellon University. Several pilots are underway using new processes. However, it will be sometime before any agencywide changes are implemented. SSA also drafted a new version of SET in February 1997 but has not adopted it as the Agency's standards. Therefore, SSA's current standards and procedures are found in the SET manual that was revised in May 1994.

SET identifies the activities that are to take place in each stage of SSA's SDLC and the products needed for documentation. SET is organized into 15 parts that are contained in 7 large volumes.

SSA's Systems Development Life Cycle

SSA's SDLC is shown in the following table.

Stage	Purpose
Planning Stage	To develop an Automated Data Processing (ADP) Plan project proposal for systems development or change, or to determine need for maintenance or minor modifications not requiring formal ADP Plan approval.
Requirements Definition and Analysis Stage	To analyze user needs and define user requirements at a level sufficiently detailed to permit system design and to develop a validation plan establishing a minimum level of acceptable performance.
Design Stage	To translate detailed functional requirements (DFR) into detailed program specifications.
Development Stage	To translate the DFR into executable computer programs.
Evaluation Stage	To verify that the functional requirements are met by the software and there are no adverse effects to the overall process.
Operational Integration and Testing Stage	To test validated application software in a production environment.
Operations Stage	To address activities taking place during the production life.
Post-implementation Review Stage	To ensure user needs are met and products perform as expected.

SCOPE AND METHODOLOGY

We used a variety of methods to achieve our objective. These included reviewing: (1) applicable laws, regulations, and guidelines; (2) OMB Circular A-130; (3) the Privacy Act of 1974; and (4) Federal Information Processing Standards Publication 106, *Guideline on Software Maintenance*.

We reviewed SET and identified pertinent products SET requires that we believed would provide documentation to meet our objective. We then selected four software projects that were completed during 1996 to determine whether they were in compliance with these provisions. Two were newly developed software - Modernized

Claims System Release 3.6 (MCS 3.6) and Drug Abuse and Alcoholism (DA&A). Two were software maintenance projects requiring cyclical updates - Benefit Rate Increase and Annual Wage Reporting for Tax Year 1995 (AWR 95). We interviewed SSA staff and reviewed the documentation prepared for the software development or maintenance for these four projects.

This review focused primarily on the first five stages of SSA's SDLC from planning through evaluation stages. The other stages will be covered in separate reports in the near future. We limited our assessment of internal controls to the required SET procedures that related to the objective of our audit. Field work was performed at SSA Headquarters in Baltimore, Maryland, from January through October 1997. We conducted this audit in accordance with generally accepted government auditing standards.

RESULTS OF REVIEW

SSA has had a comprehensive methodology for software development and maintenance since 1985 when it developed its systems engineering environment plan. The SET manual, which was part of this plan, sets forth SSA procedures. The objectives of SET are sound.[3] The findings show that because SET is difficult to use, SSA members bypassed SET procedures or substituted their own methods of documenting and controlling projects, especially when faced with stringent time frames.

In its audit of SSA's FY 1997 financial statements, PricewaterhouseCoopers reported that SSA needs to improve its software application development, change control policies and procedures, and consider this condition to be an internal control weakness under FMFIA. Our findings corroborate PricewaterhouseCoopers' concerns. Weaknesses in the software development and maintenance process increase the risk that unauthorized or untested changes could be introduced into the production environment which would reduce the reliability of the information processed. We found the following areas of concern.

AUTHORIZATIONS REQUIRED AT KEY POINTS IN THE PROCESS NEED TO BE CLEARLY DOCUMENTED

SET requires preparation of DFRs before software is designed and developed.[4] During the development process, DFRs were prepared for three of the four projects. For the software development relating to DA&A legislation, DFRs were not prepared until after the software was implemented. During the design and development phases, the functional requirements were defined in an ad hoc manner and were also relayed between components informally. The informal DFRs were 7 pages in length compared to the 133 pages of the formal DFRs that were prepared after the software was implemented. Findings show that critical information can be omitted when using an informal abbreviated document. We were informed that upper management decided to forego normal procedures because of the stringent time frames. Formal DFRs are important for several reasons. They document the service level requirements and identify audit, security, and privacy controls. They also detail the validation plan, which

[3] Part 10, Chapter 15.2 describes the objectives which include providing a vehicle for communication and providing a framework for introducing standards to ensure software usability and maintainability, maximum error detection, and improving responsiveness to user requirements.

[4] Part 30, Chapter 20.2.1.

tends to establish a level of acceptable performance. DFRs are a prerequisite for design and development stages of the SDLC and SET requires preparation of DFRs before software is designed and developed. Without this properly approved document, user needs may not be met. Without proper management control, there is risk that unauthorized or erroneous changes can be made to software, which would reduce the reliability of information processed.

SET requires preparation of a Systems Release Certification[5] (SRC) for software releases requiring a validation plan. However, for two of the four projects we reviewed, the authorizations to release the software were given orally rather than by an SRC. We believe the SRC is a key document because it shows that officials in the responsible components certify the acceptability of changes. For example, it documents the Office of Systems Requirements certification that: (1) changes have been validated; (2) validation results conform to functional requirements; (3) procedures, training, and forms have been provided to end users; (4) control, auditability, security, and privacy requirements are met; and, (5) users were notified of the implementation date. Without the signed SRC, there is no assurance that all responsible components agree that the software is ready for release.

SSA's systems life-cycle embraces an interactive team approach to systems development. According to SET, users are to be substantially involved in the planning phase.[6] They are responsible for the user planning team report with recommendations, which is a management decisionmaking document. This documentation was not available for the two new software releases we reviewed. We did note that a core group was convened for the DA&A software process. However, the core group substituted their own control and tracking methods, and instead of issuing a team report, developed an issue and resolutions chart. Without a defined and consistent process, there is no assurance that all important documentation and authorizations will be obtained. Properly authorized documentation is essential to protect against erroneous changes and weakened security controls. These documents should be maintained for as long as a system is in operation in case questions arise regarding why or when certain modifications were adopted.

ESSENTIAL DOCUMENTS NEED TO BE KEPT IN A CENTRAL REPOSITORY

There was no central repository for essential documents making retrieval difficult and time consuming. For the four projects, we were not able to go to one location to obtain project documentation. We were referred to multiple components and several staff

[5] Part 60, Chapter 30.7.

[6] Part 20, Chapter 30.2.3.

members before we could determine if a document had been prepared and could be obtained, if it existed. For example, we had to contact five people in three components to determine whether there was an SRC for the DA&A software releases and how authorization was given. Easy retrieval of important documents is essential for the integrity and maintainability of software. Properly authorized documents should be kept in one central place and remain readily available for review while an application is in operation.

CRITICAL PROBLEMS IDENTIFIED DURING VALIDATION NEED TO BE RESOLVED

SET requires that problems found during validation be reported and resolved. If the problems are not resolved, an estimate is to be prepared of their effect on the system, the public, and SSA's operating components.[7] SET requires that an analysis be made of unresolved errors to determine if the level of a problem is within acceptable tolerances. We believe this is an important standard to ensure the integrity of software and one that should not be compromised. However, we found that for two of the four systems reviewed, software that contained critical problems was released to production.

- Because of the pressure to meet target dates, software modifications were released for AWR 95 with 7 critical problems and 17 high-priority problems unresolved. Because of these problems, several workloads in operating components had to be interrupted until the software problems were resolved. Moreover, we believe this situation increased the risk of erroneous data being processed to earnings records. For example, the validation process identified two records that did not correctly reflect domestic service or tip wages. One record reflected wages of $21,693 that should have been $19,565. Another reflected wages of $17,893 that should have been $15,997. Without correcting problems identified during the validation process, incorrect benefits could be paid, such as overpayments for these records.

- Software for MCS 3.6 was released with two high-priority problems unresolved. One problem affected the amount of benefit payment because the worker's compensation offset was not always applied correctly. The validation process for MCS 3.6 identified a case where the software failed to reduce a beneficiary's monthly benefit by $124.20 to offset the worker's compensation he was receiving. This problem was reported on November 7, 1996, and again on November 25, 1996. Nevertheless, the software was implemented on December 9, 1996. As of August 1997, 8 months after the MCS 3.6 software was implemented, the problem still had not been resolved because the cause of the problem could not be identified. This problem could cause incorrect monthly benefit payments and create overpayments. SSA did not analyze the number of

[7] Part 60, Chapter 30.6.2.5.

beneficiaries that may be affected or the amount of overpayments that may occur to determine whether the problem was within an acceptable tolerance. This is another example where unresolved problems could affect one of SSA's primary missions, that of paying beneficiaries correctly.

- Another problem associated with MCS 3.6 affected information on notices sent to beneficiaries who filed for benefits under their own SSN (earnings record) and also on the earnings record of their spouse. Notices for these cases were not explaining the basis for the benefit calculation. The notices needed to explain which earnings record provided the largest benefit. This condition was reported on December 4, 1996, but a decision was made not to correct it until the scheduled release of MCS 3.6.1 software in August 1997. SSA made this decision because it believed difficulties would be encountered in validating a maintenance release. Not resolving problems such as this will affect SSA's goal of providing clear notices to the public.

QUALITY ASSURANCE REVIEWS SHOULD BE PERFORMED

SET states that the quality assurance process must ensure systems development standards are in place, and, when they are used, they produce products that meet requirements and are fit for use. The objective of the quality assurance program must be to produce products that are free of defects.[8] The Office of Systems Planning and Integration (OSPI) is responsible for quality assurance. We contacted staff from OSPI to determine whether the projects selected for our review were also selected for SSA's quality assurance reviews. OSPI staff informed us that no quality assurance reviews had been performed in more than 2 years because resources were focused on piloting methodologies for the future. As our review revealed, without monitoring and enforcement of standards, the quality assurance objective of SET is not being met. As a result, beneficiaries may not receive world-class service and may be paid incorrectly.

[8] Part 110, Chapter 10.

CONCLUSIONS AND RECOMMENDATIONS

We concluded that discipline and consistency in SSA's current systems development and maintenance process has deteriorated for several reasons. SET is difficult to use, especially in today's dynamic systems environment. Also, it does not clearly differentiate between mandatory standards and discretionary guidelines. In addition, we believe SSA is focused on piloting methodologies for the future and is no longer enforcing current standards. SSA needs to establish an organizational commitment to restoring consistency and discipline in its present process while it plans for the future.

We recommend that SSA:

1. Enforce the requirements for authorizations and documentation at key points in the SDLC.

2. Establish procedures in SET for maintaining critical documents in a central repository.

3. Enforce the requirement that high priority problems discovered during validation be resolved before the software is released to production.

4. Reinstate quality assurance reviews prescribed in SET.

SSA agreed with our recommendations. Currently SSA is implementing projects relating to our first two recommendations. In response to our third recommendation, SSA stated that it will when possible, remove changes where problems have occurred and implement the changes in a later release. Finally, SSA stated that it plans to reinstate quality assurance reviews and is piloting integrated quality assurance reviews within the framework of CMM. Appendix A includes a copy of the complete text of SSA's comments.

APPENDICES

APPENDIX A

SSA COMMENTS

MAJOR CONTRIBUTORS TO THIS REPORT

Office of the Inspector General

Don Franklin, Director, Systems Audits

Bruce Daugherty, Audit Manager

Jean Lynch, Senior Auditor

Randy Townsley, Senior Auditor

Greg Hungerman, Program Analyst

Harold Hunter, Senior Auditor

For additional copies of this report, please contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-9135. Refer to Common Identification Number A-13-96-11000.

SSA ORGANIZATIONAL CHART