The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made

January 2002

Reference Number: 2002-20-044

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

January 31, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made (Audit # 200020003)

This report presents the results of our review of the system-level controls over the Internal Revenue Service's (IRS) Security and Communications System (SACS). The overall objective of this review was to assess the IRS' progress in meeting appropriate security requirements for the SACS and to evaluate the controls over system access, operating system changes, and service continuity.

The SACS is a critical component of the IRS' customer service efforts, providing front-end access and security services to mission critical systems, including the Integrated Data Retrieval System (IDRS). Strong system-level access controls are needed in the SACS environment to ensure that the IDRS is available for use in answering taxpayer inquiries and that taxpayer burden is minimized when contacting the IRS. From January through September 2001, an average of 26.4 million individual and business tax accounts were available per week for inquiry on the IDRS.

In summary, we found that an adequate change control process has been implemented for the SACS and steps are being taken to improve the system level access controls in the SACS environment. However, several weaknesses were identified in the areas of system documentation and system access controls. Specifically, planned actions to develop a technical configuration database need to be completed. Also, system design documentation has not been developed for the SACS security system. Regarding system-level access controls, we identified weaknesses that granted users greater access to the SACS mainframes than needed for their job responsibilities. In addition, access controls for SACS console support systems do not meet IRS requirements. In the service continuity area, we determined that the controls for the SACS environment are adequate to ensure that necessary personnel are prepared to react appropriately in case of a service interruption. In addition, we determined that the staff complies with the established "fallback" procedures in case of a system interruption.

Based on our audit work, we identified several steps that the Chief, Information Technology Services (ITS) should take to improve the controls over the SACS system. We recommended that the Chief, ITS ensure that SACS system baseline information is formally approved and maintained and that design documentation be developed and maintained for the SACS security system. Also, steps should be taken to improve the security oversight of the SACS environment. Specifically, we recommended the revision of existing access standards and development of new access standards for the SACS environment and that the SACS security system be modified to restrict user profiles to an appropriate level of access. In addition, IDRS security reports should be reviewed to ensure that only SACS security administrators have access to the IDRS command code used for SACS mainframe user security administration. Regarding the SACS console support systems, we recommended that the security administration responsibilities for these systems be reassigned to an independent security function.

Management's Response: IRS management agreed with the recommendations presented in the report. Corrective actions will be taken to improve system documentation, security oversight, and access controls over the system. Management's complete response to the draft report is included as Appendix IV.

The Treasury Inspector General for Tax Administration has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the Treasury Inspector General for Tax Administration's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made

Background

The Security and Communications System (SACS) is a critical component of the IRS' customer service efforts, providing front-end access and security services to the following mission critical systems:

- Integrated Data Retrieval System (IDRS): The IDRS enables designated IRS employees to have instantaneous visual access to certain taxpayer accounts. The SACS manages the communications workload and provides access control, audit logging, terminal authentication, and user authentication security services for the IDRS.
- Corporate Files On-Line (CFOL): The CFOL system provides immediate on-line access to taxpayer information residing at the Martinsburg Computing Center (MCC). The SACS also controls access to the CFOL system.

Strong system-level access controls are needed in the SACS environment to ensure that the IDRS is available for use in answering taxpayer inquiries and that taxpayer burden is minimized when contacting the IRS. In addition, strong controls are needed to ensure that taxpayer information processed through and stored in the SACS environment is adequately protected from unauthorized access or alteration. From January through September 2001, an average of 26.4 million individual and business tax accounts were available per week for inquiry on the IDRS.

(b)(7)(E)

[1] Integrated Collection System (ICS) /Automated Collection System (ACS) /Printer Replacement to Integrate New Tools (PRINT)

(b)(7)(E)

(b)(7)(E)

Through our evaluation of the system-level security of the SACS environment, this review addresses the IRS' strategic goal of implementing a comprehensive program to address internal and external privacy and security. This goal includes the priorities of formulating an IRS-wide approach to protect taxpayer data and establishing appropriate electronic security.

Audit work was performed on-site at the MCC and TCC as well as at the IRS' National Headquarters in the offices of the Chief, Information Technology Services, from February 2001 to October 2001 as part of our Fiscal Year 2001 Annual Audit Plan. The audit was performed in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Although an Adequate Change Control Process Has Been Implemented for the SACS Mainframe, System Baseline Information Needs To Be Approved and Maintained

The purpose of a formal configuration management process is to provide a controlled, repeatable process for the handling of all system products or deliverables within the domain of an organization. The configuration management process is a control that should prevent changes from being made to the system that unintentionally or unknowingly diminish security or systems availability.

To provide structure in its configuration management processes, the IRS' Systems Support Division (SSD) has developed the SSD Configuration Management (CM) Handbook. This handbook provides guidance regarding the implementation of a change control process for the computer systems under the responsibility of the division. The handbook establishes a change request/transmittal system to document and control system changes. The handbook details the roles and responsibilities of each key position in processing system changes.

The SSD has implemented many of the processes outlined in the configuration handbook for the SACS environment. All changes to the SACS environment are documented through online change requests and managed by the SSD Change Control Board. This Board meets regularly to review and approve changes for all systems supported by the SSD. To facilitate its change control process, the SSD has made effective use of its website to provide status information on proposed change requests as they move through the approval process.

However, in our review of the SSD configuration management processes, we could not identify formally approved system baselines.[2] The SSD CM Handbook requires the development and maintenance of two formal baselines (production and contingency baselines).

The SSD is sponsoring the development of a Technical Configuration Data Base (TCDB) prototype, which will be used as a centralized repository (CM Library) for the SSD commercial off-the-shelf software baseline. There is no timetable for completion of this database. The SSD believes the establishment of a "formal baseline" is dependent on the establishment of the TCDB with current and accurate data.

The SSD has implemented interim processes for documenting "informal" system baselines for the SACS environment while it is in the process of developing a formal process. In our review of system change documentation and in discussions with SACS personnel, we determined that they are using the SSD transmittal system

[2] A baseline is a "point in time collection" of work products and other documentation that has been formally reviewed and agreed upon, serves as the basis for further development and can only be changed through formal change control procedures.

as the means of documenting changes to and maintaining the current system parameters. As system changes are made, the transmittal system is relied upon to capture each change and reflect the current system characteristics. By using the transmittal system rather than maintaining the system requirements or parameters in a baseline document or database, significant manual effort is required to capture the current system parameters. Each individual transmittal must be examined to determine what system parameter is addressed, how it has been altered, and why it was altered.

Recommendation

1. The Chief, Information Technology Services, should ensure the SACS system baseline information is formally approved and maintained, as required by the SSD CM Handbook.

Management's Response: The Security Systems Software Section will develop a baseline document and present it to the Director, SSD for formal approval. The Security Systems Software Section will continue to maintain the baseline document in accordance with the Change Control Board and Change Management Process.

Design Documentation for the SACS Security System Has Not Been Developed

The IRS' Information System Security Procedural Guide, IRS Document 9627, provides standardized procedures to be used by IRS organizations to ensure the protection of sensitive but unclassified information systems, applications, and networks. This document provides procedures for the development of system documentation, including a Computer Security Plan, Risk Assessment, and Trusted Facility Manual.

The IRS met these standards in its preparation of the Risk Assessment, Computer Security Plan, and Trusted Facility Manual for the SACS mainframes. However, system design documentation has not been prepared for the system-level security system residing on SACS mainframes In 1994, when the SACS security system was implemented on the SACS' predecessor system, the Communications Replacement System, an initial system baseline documenting the system's design and requirements was not created. SSD personnel were not able to identify why this key step was not completed.

The IRS' Information System Security Procedural Guide states the purpose of the design documentation is to identify and describe the system and its security features. Specifically, the design documentation should:

- Explain the system's protection mechanisms so that the effect a change may have on the security of the system can be evaluated prior to a change being performed.
- Facilitate the system administrators in modifying and maintaining the system throughout its life-cycle, without compromising the trustworthiness of the system.
- Present a technical history of the system, containing documentation on changes to the system.
- Provide enough detail to serve as a useful tool for maintenance of the system.
- Clearly indicate what elements of the design impact the trustworthiness of the system.

This guide also states that the design documentation should be current throughout the entire life cycle of the system. All changes made to the system should result in a change to the design documentation.

Normally, access control software for a mainframe system is purchased from a vendor along with accompanying design documentation. The vendor typically develops the system requirements and publishes reference documentation describing the requirements of the system. This reference documentation describes in detail the appropriate steps needed to maintain the system and provides information needed to evaluate modifications to the system.

However, because vendor-developed access control software was not useable for the SACS mainframes, IRS personnel developed the TPF security system residing on the SACS mainframe. In such an "in-house" development, documentation of system requirements is imperative since this documentation provides the basis for evaluating the impact of proposed modifications. In addition, the documentation also provides system history information that would allow an outside source to provide system maintenance.

Without this documentation, knowledge of the security system resides solely with the staff responsible for the system. For SACS, the systems programming staff in the SSD currently consists of 21 staff members (including 6 contractors) who are responsible for the SACS environment. If the IRS were to lose these employees, it would be extremely difficult for their knowledge and expertise to be replaced in the absence of adequate documentation. It would also be problematic for an external organization to make an adequate assessment of the security system without design documentation.

Recommendation

2. The Chief, Information Technology Services, should ensure system design documentation is developed and maintained for the security system residing on the SACS mainframes, as required by IRS Document 9627.

Management's Response: The Security Systems Software Section will develop a system design document and present it to the Director, SSD for formal approval. The Security Systems Software Section will maintain the system design documentation in accordance with the Change Control Board and Change Management Process.

The IRS Is Taking Steps To Improve System-Level Access Controls in the SACS Environment

System-level access controls should provide reasonable assurance that computer systems, including system-level software, application programs and data, are protected against unauthorized modification and disclosure. Our review found that the IRS has appropriately controlled access to most of the critical components in the SACS environment. Among the access controls that the IRS has adequately configured are those over the source code for the programs used on the SACS mainframes, with access restricted to SACS systems programmers. In addition, remote access to the SACS mainframes through network services has been appropriately disabled. On the EOCF systems supporting the SACS mainframes, user profiles are appropriately assigned.

During our review, several areas were identified where improvements to the (b)(7)(E) [redacted] are needed, and which IRS management is addressing. These improvements will enhance the IRS' (b)(7)(E) [redacted] In addition, these improvements will enable the IRS to (b)(7)(E) [redacted] Specific details regarding the improvements to the (b)(7)(E) [redacted] are provided below.

(b)(7)(E) [redacted]

The IRS is currently taking action to add security features to (b)(7)(E) [redacted] In April 2001, change requests were submitted and have been subsequently approved to develop the following (b)(7)(E) [redacted]

- (b)(7)(E) [redacted]
- (b)(7)(E) [redacted]
- (b)(7)(E) [redacted]
- (b)(7)(E) [redacted]

Access control weaknesses identified during the review and addressed by the IRS

During our review, we identified several instances where either IRS policies were not followed or access controls could be improved in the SACS environment. We informed IRS management of these issues, who in response took corrective action to address them. Specifically, we found the following:

- While the process for requesting and granting user access to the SACS mainframes is working properly, several instances were identified where the process for timely removing user access was not followed. Specifically, five users were identified with access to the SACS mainframes who had either been reassigned to other projects or no longer worked for the IRS. The IRS uses Form 5081, "Information Systems User Registration/Change Request," to administer access to its computer systems. According to the MCC SACS security administrators, access for these users was not timely revoked since formal notification, through IRS Form 5081, was not received by the MCC security personnel. After we notified MCC security personnel of these users, their access was removed.
- (b)(7)(E) [redacted]
- (b)(7)(E) [redacted]

(b)(7)(E) [redacted]

- An excessive number of users, 57, from the TCC were granted access to the MCC production SACS mainframe for backup purposes. The existence of these users will create an additional burden on the MCC SACS security administrators, once the security mechanism to disable inactive users is added to the SACS mainframes. At that point, MCC SACS administrators will need to periodically re-activate all 57 users since they will not be regularly accessing the MCC SACS mainframe. We reported this issue to the appropriate TCC security and operations personnel, who reduced the number of users on the MCC production SACS mainframe to eight.

Security administration improvement

Our review also identified that two users were mistakenly assigned the command code used to administer system-level security on the SACS mainframes. (b)(7)(E) [redacted] The assignment of this code should be restricted to SACS security administrators to prevent accidental or unauthorized addition, modification, or deletion of SACS mainframe user profiles. During the review we identified that two of the six users granted access to this code were not SACS security administrators. In our discussions with the IDRS security administrator for these users, we determined that they were inadvertently assigned the code when granted access to the IDRS.

The IRS generates monthly security reports for its IDRS security personnel (IDRS groups 930 and 931), which are the only groups with access to the (b)(7)(E) [redacted] and other IDRS security command codes. This report lists the users in each group and the IDRS security command codes to which they have access. However, the unauthorized users were identified only after we requested a special report listing all users with access to the (b)(7)(E) command code. Upon seeing this report, IDRS security personnel removed the command code from the profiles of the two unauthorized users.

Recommendation

3. The Chief, Information Technology Services, should ensure that monthly IDRS reports for security personnel (groups 930 and 931) are reviewed to ensure that only SACS security administrators have access to the IDRS command code used to administer system-level access to the SACS mainframes.

Management's Response: The Office of Security Evaluation and Oversight (SEO) will issue a memo to the Data Security Chiefs advising that the IDRS command code used to administer system-level access to the SACS mainframes is not to be included in the Data Security Employee Profiles. Any deviation from this procedure, such as to support TCC and MCC Security Administrators, will require approval. Also, the memo will address that this command code is not to be included in the Unit Command Code Profile for either IDRS security personnel units 930 or 931. This will reiterate the current Law Enforcement Manual.

Users Have Profiles in the SACS Environment With Greater Access Than Necessary

In the SACS environment, user profiles specify the commands and files that users can access. For the SACS mainframes, system users are assigned one of six profiles based on their job responsibilities. These profiles are established through the IRS-developed security system for the SACS mainframes. Through these profiles, users can, for example, issue system commands to alter core system programs, perform operator functions, and manage network connectivity. For the SACS related files on the IAP mainframes, users are granted access through profiles defined in the OS/390 security server for those files. These files include a variety of sensitive taxpayer information, such as IDRS audit trail records and reports, as well as IRS employee information.

Our review of the user profiles for the SACS environment identified several weaknesses that granted users greater access to the SACS mainframes than needed for their job responsibilities. Such access contradicts information system security principles of "least privilege," as outlined in the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and in the Trusted Facility Manual (TFM) for the Service Center Support System (SCSS), which includes the SACS and IAP mainframes. This principle requires that "users are granted enough privilege or access authority to perform assigned tasks, but no more – the least privilege needed to perform a job."

Specifically, our review of the user profiles for the **SACS mainframes** identified the following:

- Review of the system operator command table on the SACS mainframes identified two user profiles that were granted access to significantly more SACS system commands than outlined in the SACS access standards. Currently, these profiles are granted access to nearly all SACS system commands; however, the SACS access standards, issued in July 1994, provided that these two profiles be granted access to relatively few system commands. According to the SACS systems programmers, this oversight resulted from a misunderstanding of the purpose of the console profiles by the systems programmer responsible for maintaining them.
- At the time of our review, there were 222 users with access to one or more of the SACS mainframes. Our analysis of the profiles assigned to these users identified that 149 users were granted profiles that were appropriate for the users' job responsibilities. In addition, 60 users had job titles that did not match those of the available profiles and therefore their appropriateness could not be determined. However, the remaining 13 users were assigned profiles inconsistent with their job responsibilities. Specifically, these users were assigned profiles with greater access than their job

responsibilities required. SACS security personnel were notified of these exceptions and appropriately corrected 8 of the 13 user profiles. The other five profiles that need to be corrected are for SSD and TCC users granted restricted SACS system programmer profiles.

Granting users greater access than necessary could lead to inadvertent actions that result in a system shutdown of the SACS mainframes. (b)(7)(E)

Our review of user profiles for SACS-related datasets on the **IAP mainframes**, defined through the OS/390 security server, identified the following instances of inappropriate or excessive access authority:

- There are 113 users that can update or alter SACS-related production files containing sensitive information, such as IDRS audit trail, cumulative command code usage, and employee reference data. Similarly, 89 users can update or alter similar information used for development of SACS programs. While several system UserIDs are granted access to this information, most users are computer operations and programming personnel. According to the SACS systems programming personnel, only system UserIDs that create and/or process this data should be granted this level of access.

- In addition, there are 194 users who can update or alter SACS-related production files containing other sensitive information, such as IRS employee social security number (SSN) information as well as various IDRS reports.

Granting users the ability to alter or update IDRS audit trail information and reports as well as employee information could result in unauthorized access of taxpayer information. Such access could lead to the intentional viewing and/or modifying of taxpayer-related information. In addition, the potential exists for users to either purposefully or unintentionally delete these datasets.

The conditions identified on both the SACS and IAP mainframes occurred in part due to the incomplete and outdated access standards for the SACS environment. Specifically, the following shortcomings in the standards were identified:

- The access standards have not been updated to reflect the changes to user profiles since they were issued in July 1994. Since 1994, there have been 160 commands added to the user profiles on the SACS mainframes. Consequently, the standards do not provide adequate guidance on the system commands each user profile should be granted on the SACS mainframes. In addition, the standards do not include guidance on new security features added to the SACS mainframes after the standards were issued, such as the exclusion of designated operator commands from the SACS system audit trail. Such guidance would help ensure that these new features are properly configured.

- The existing standards do not specify how some users should be profiled on the SACS mainframes. The standards provide profiles for six types of users, such as operators and systems programmers. However, there is no guidance for assigning profiles to users other than for the types specified in the standards In addition, the standards do not provide the types of commands granted to each profile, such as alter, display, and system commands. Consequently, such users may be granted a profile that provides a higher level of access than needed.

- The existing standards do not incorporate any guidance on how to administer the SACS-related files on the IAP mainframes. Such guidance is needed to assist the IAP mainframe security administrators in properly securing SACS-related files by identifying the purpose of the files and specifying the types of users who should have access and their level of access.

For its other mainframe environments, the IRS has prepared detailed access standards and guidelines for the security administration over those systems. In addition, the standards provide a process for requesting a deviation from the standards in special situations. For the SACS environment, no such deviation process has been outlined.

Recommendations

4. The Chief, Information Technology Services, should ensure that the system operator command table for the SACS mainframes be modified to restrict user profiles to an appropriate level of access.

   Management's Response: The SEO will assist the SSD in reviewing the operator command table and in adjusting user profiles and established authorities, with the assistance of the computing centers. The SEO will submit any necessary change requests for the establishment of appropriate user profiles. The revised profiles will then be assigned by the computing centers to the appropriate officials.

5. The Chief, Information Technology Services, should ensure the Directors, TCC and SSD take action to ensure that all users with restricted systems programmer profiles on the SACS mainframes are brought into compliance with the SACS access standards or request approval from the Office of Security, Evaluation, and Oversight to deviate from the access standards for these users.

   Management's Response: In addition to the corrective actions in response to Recommendation 4, the SEO will issue interim guidelines, standards, and procedures.

6. The Chief, Information Technology Services, should revise the access control standard documentation for the SACS environment to include: new and/or updated information on the SACS operator commands; guidance to assist SACS security administrators in assigning appropriate SACS profiles to users; and access standards for the SACS-related datasets on the IAP mainframes. These standards should also include a waiver process similar to ones in place for other IRS mainframe environments.

Management's Response: The SEO will assist the Security Systems Software Section in revising the access control standard documentation for the SACS environment, including references to the SACS-related datasets on the IAP mainframes. The actual standards for these datasets are included in the IAP Access Matrix. The SACS access control standard documentation will also include a waiver process similar to that documented for use in other IRS systems. This documentation, however, cannot be completed until all required actions are taken on the SACS, including those currently scheduled for completion in July 2002.

7. The Chief, Information Technology Services, should ensure the Directors, MCC and TCC take action to ensure that the SACS environment is compliant with the revised SACS access control standards once they have been prepared.

   Management's Response: Action will be taken by the Director, Enterprise Operations to ensure the SACS environment is compliant with the revised SACS access control standards once they are completed. This action is dependent upon the issuance of SACS access control Guidelines, Standards, and Procedures (GSPs) by the SEO and their implementation.

Several Access Controls for the EOCF Systems Do Not Meet IRS Requirements

As discussed previously, [redacted] (b)(7)(E)

Our review of the access controls over these systems identified that they do not meet several of the IRS' computer security policies, which are discussed below. The EOCF systems facilitate user access to the SACS mainframes as well as provide automation and remote access to SACS systems programmers. Consequently, any compromise or misuse of these systems could decrease the efficiency of the operation of the SACS mainframes.

Specifically, our review of the EOCF systems identified the following:

- IRS policies require that all user access requests to its information systems be documented and approved using Form 5081. However, at the time of our review, only 23 of the 157 users with access to EOCF systems had submitted an authorization form. Users were previously added to EOCF systems from a list of users supplied by the MCC and TCC, at the request of SACS systems programmers. The SACS systems programmers recognized this omission after the start of our review and completed the EOCF access user re-certification process using Form 5081 in August 2001. All users that were not re-certified during the period were removed from the EOCF system(s).
- (b)(7)(E)
- IRS policies also require the creation of user and system activity reports, from system audit trails, and their distribution to appropriate managers for review. While the EOCF system logs record user and system activity, which are archived on a daily basis, no reports are generated for management review.

These conditions result, in part, from the fact that the SACS systems programmers administer security for the EOCF systems. While the systems programmers have significant experience with the EOCF systems, they do not necessarily have experience in security administration policies and procedures. This is most evident in the deficiencies identified with granting access to EOCF systems and generating audit trail reports. Since there are inherent limitations of the EOCF security system, the IRS needs to ensure that there are compensating controls and an effective security administration program in place to deter and/or detect any compromise of EOCF systems.

Recommendations

8. The Chief, Information Technology Services should develop access standards for the EOCF systems that specify guidelines and requirements for use by security personnel in administering the EOCF systems.

   Management's Response: The SEO will assist the Security Systems Software Section in developing access standards and security administration documentation for the EOCF systems. Once completed, this documentation will be provided to security administrators at the computing centers.

9. The Chief, Information Technology Services should reassign security administration responsibilities for the EOCF systems to an independent security function, such as the security functions in the MCC and TCC.

   Management's Response: The Security Systems Software Section will provide training and transfer security responsibilities for the EOCF to the computing centers upon completion of the pending Modernization and Information Technology Services organizational realignment.

10. The Chief, Information Technology Services should ensure that EOCF user access is annually re-certified and that audit trail reports on user activity are generated weekly and distributed to user management for review.

    Management's Response: The Systems Software Branch completed EOCF user access re-certification. The SEO will establish a task force to evaluate and review the lack of weekly generated and distributed EOCF audit trail reports and propose a solution.

Service Continuity Controls Are Adequate

All computer systems need to have controls in place to ensure that the services provided by these systems are available when needed. A prolonged loss of these services can significantly affect an organization's ability to accomplish its mission. This is especially true for the SACS environment, since it processes hundreds of transactions per second and quick response time to the IDRS and CFOL is needed to enable the IRS to timely respond to taxpayer inquires. As a result, strong service continuity controls need to be in place to ensure that the SACS mainframes are operating and available to support the IRS' ability to provide timely customer service to taxpayers.

Our review of the service continuity controls for the SACS environment determined that they are adequate to ensure that necessary personnel are prepared to react appropriately in case of a service interruption. In addition, we determined that the staff complies with the established "fallback" procedures in case of a system interruption, of which there have been relatively few during the past year.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the Internal Revenue Service's (IRS) progress in meeting appropriate security requirements for the Security and Communications System (SACS) and to evaluate the controls over system access, operating system changes, and service continuity. The audit was conducted as part of our annual audit plan. To complete this objective, we:

I. Assessed the adequacy and timeliness of the SACS system-security and system documentation and procedures.

A. Assessed the adequacy and timeliness of documentation required for the SACS certification.

1. Reviewed the current risk assessment for the IRS' consolidated mainframe systems, which includes SACS, to ensure that vulnerabilities were identified and mitigated.
2. Reviewed the security plan for the IRS' consolidated mainframe systems, which includes SACS, to ensure it was current and covered all major components and included topics prescribed by Office of Management and Budget (OMB) Circular A-130.
3. Reviewed the Trusted Facility Manual for the locations where the SACS is physically located and/or where sensitive access is permitted to ensure that information regarding SACS is current and reflected any recent changes to the system.

B. Assessed the adequacy and timeliness of SACS security procedures.

1. Determined if a Law Enforcement Manual (LEM), or equivalent documentation had been developed for SACS.
2. Determined if access control standards (i.e., control matrix) had been developed for SACS.
3. Identified any other security documentation developed for SACS.
4. Determined whether security documentation developed by non-security personnel had been evaluated by the Office of Security, Evaluation, and Oversight.
5. Determined whether all security documentation was periodically reviewed, approved by management and kept current.

- C. Assessed the completeness and timeliness of system-security analysis and design documentation for SACS.
  1. Determined whether analysis and design documentation for SACS included requirements for the IRS-developed console security system for SACS.
  2. Determined whether this documentation was complete, kept current, and approved by appropriate management, especially the Office of Security, Evaluation, and Oversight.

II. Determined whether access controls to system-level resources provided reasonable assurance that data files, application programs, and computer-based facilities and equipment were protected against unauthorized modification, disclosure, loss, or impairment.

- A. Assessed the policies and procedures in place for authorizing and documenting access to information resources by determining whether:
  1. Resource owners had identified authorized users and their authorized level of access.
  2. Emergency and temporary access authorization was controlled.
  3. Owners determined disposition and sharing of data.
- B. Determined if adequate physical security controls had been implemented over the transfer of tapes between IRS systems by determining whether:
  1. Adequate controls were in place to prevent accidental loss of data on batch tapes while being transferred from SACS to the point of printout and distribution. This path included tape transfer between the SACS and Integrated Collection System (ICS) /Automated Collection System (ACS) /Printer Replacement to Integrate New Tools (PRINT) (IAP) mainframes.
  2. Adequate controls were in place over console access at the New Carrolton Federal Building.
- C. Evaluated the implementation of logical access controls on SACS, IAP relevant Logical Partitions, and the Extended Operating Console Facility (EOCF) system, by determining if:
  1. Passwords, tokens, or other devices were used to identify and authenticate users.
  2. An analysis of the logical access paths was performed whenever changes to the system were made.
  3. Logical controls were in place to restrict access to production, test, and batch libraries.
  4. Logical controls were in place to restrict access to and modification of security software programs and files.
  5. Adequate separation of duties was maintained in the assignment of user profiles.

6. Logical controls over the Integrated Data Retrieval System (IDRS) command code, terminal, and access tables were in place.
7. Logical controls over telecommunications access were in place.

D. Determined if system-level audit trails were maintained, identifying that all activity involving access to and modifications of sensitive or critical files was logged.

1. Determined if actual or attempted unauthorized, unusual, or sensitive access was monitored
2. Determined if suspicious access activity was investigated and appropriate action taken.

III. Assessed the adequacy of the process for making changes to the SACS operating system environment. This audit step did not include changes to the IDRS security system which is the major application running on SACS.

A. Evaluated the review and authorization of requests for changes to the SACS operating system environment.

1. Assessed the use of the Computer Associates (CA) Endevor software (CA-Endevor) in the configuration management process.
2. Reviewed a random judgmental sample of transmittal logs for SACS from January 2000 through April 2001 to determine if changes implemented corresponded to changes documented and approved.
3. Determined whether there was required change request documentation for the sampled transmittals.

B. Examined the testing process implemented to evaluate proposed system changes to the SACS.

1. Assessed the policies and procedures governing the testing process.
2. Determined how access to the Transaction Processing Facility (TPF) system and IAP test libraries was controlled.
3. Determined how access to the TPF system and IAP test libraries was monitored.
4. Reviewed a sample of implemented transmittals for adequate testing documentation.

C. Evaluated the procedures in place for implementing emergency system updates.

1. Assessed the policies and procedures governing emergency updates. This included any type of patch applied at the operating system level.
2. Reviewed testing documentation submitted with change requests categorized as "Priority 1 - Critical" to ensure that documentation of these changes was prepared in a timely manner after implementation.

IV. Evaluated the service continuity controls in place for the SACS.

A. Assessed the extent of previous SACS processing interruptions. Key points included:

1. Evaluating problem tickets created in response to service interruptions.
2. Interviewing Computer Systems Analysts, Operators, and Capacity Management personnel to identify instances where SACS had experienced significant downtime.

B. Evaluated the procedures in place to mitigate service interruptions. Key points included:

1. Evaluating the restoration procedures for security (i.e., system and IDRS) files and programs.
2. Determining whether there had been significant problems with running the backup and recovery procedures when the system has gone down.

C. Determined if the service continuity procedures in place had been adequately tested.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Vincent Dell'Orto, Audit Manager
Kevin Burke, Senior Auditor
Myron Gulley, Senior Auditor
Mike Howard, Senior Auditor
Olivia Jasper, Auditor

Appendix III

Report Distribution List

Chief, Information Technology Services M:I
Director, Office of Security M:S
Director, Corporate Computing M:I:E
Director, Martinsburg Computing Center M:I:E:MC
Director, Tennessee Computing Center M:I:E:TC
Director, Systems Support Division M:I:E:SS
Deputy Chief Financial Officer, Department of the Treasury

TD P 15-71

Appendix IV

Management's Response to the Draft Report

LIMITED OFFICIAL USE
DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D C. 20224

EPUTY COMMISSIONER

January 11, 2002

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT: Response to Draft Report – The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made (Audit # 200220003)

Thank you for the opportunity to review and comment on your draft report and recommendations concerning the Security and Communications System (SACS).

In your report, you stated that the system-level controls over the SACS are generally adequate; however, improvements can be made in system documentation and system access controls. It is our management goal to continually strive for an enhanced security program that effectively manages risks. In that regard, we appreciate your comments that will further assist us in strengthening our security controls. See the attached detailed response to each of your report recommendations.

If you have any questions or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of Security at (202) 622-8910.

Attachment

LIMITED OFFICIAL USE

TD P 15-71

Management Response to Draft Audit Report - The System-Level Controls Over the Security and Communications System (SACS) Are Adequate; However, Improvements Can Be Made (Audit #20020003)

RECOMMENDATION #1:

The Chief, Information Technology Services, should ensure the SACS system baseline information is formally approved and maintained, as required by the SSD CM Handbook.

ASSESSMENT OF CAUSE:

Section was not aware of requirement for formal approval at the time of Consolidation.

CORRECTIVE ACTION(S) TO RECOMMENDATION #1:

1a. A baseline document will be developed by the Security Systems Software Section and presented to the Director, Systems Support Division for formal approval.

1b. The Security Systems Software Section, of the Systems Software Branch, will continue to maintain the baseline document in accordance with Change Control Board and Change Management Process.

IMPLEMENTATION DATE(S):

1a. December 1, 2002

1b. Completed -- On-going

RESPONSIBLE OFFICIAL(S):

1a. Chief, IBM Systems Software Branch, M:I:SS:IS

1b. Chief, IBM Systems Software Branch, M:I:SS:IS

RECOMMENDATION #2:

The Chief, Information Technology Services, should ensure system design documentation is developed and maintained for the security system residing on the SACS mainframes, as required by IRS Document 9627.

ASSESSMENT OF CAUSE:

Insufficient system design documentation for Transaction Processing Facility (TPF) console security.

CORRECTIVE ACTION(S) TO RECOMMENDATION #2:

1a. A system design document will be developed by the Security System Software Section and presented to the Director, Systems Support Division for formal approval.

1b. The Security Systems Software Section, of the Systems Software Branch, will continue to maintain the system design documentation in accordance with Change Control Board and Change Management Process.

IMPLEMENTATION DATE(S):

1a. December 1, 2002

1b. Completed – On-going

RESPONSIBLE OFFICIAL(S)

1a. Chief, IBM Systems Software Branch, M:I:SS:IS

1b. Chief, IBM Systems Software Branch, M:I:SS:IS

RECOMMENDATION #3:

The Chief, Information Technology Services, should ensure that monthly Integrated Data Retrieval System (IDRS) reports for security personnel (groups 930 and 931) are reviewed to ensure that only SACS security administrators have access to the IDRS command code used to administer system-level access to the SACS mainframes.

ASSESSMENT OF CAUSE:

The command code b)(7)(E) was in several service center profiles that did not need or use the command.

CORRECTIVE ACTION(S) TO RECOMMENDATION #3:

The Office of Security Evaluation and Oversight will issue a memo to the Data Security Chiefs advising that b)(7)(E) is not to be included in the Data Security Employee Profiles. Any deviation from this procedure, such as to support TCC and MCC Security Administrators, will require approval. Also, the memo will address that the IDRS command code b)(7)(E) is not to be included in the Unit Command Code Profile for either IDRS security personnel units 930 or 931. This will reiterate the current Law Enforcement Manual (LEM) 25.10.3, Section 3.24.

IMPLEMENTATION DATE(S):

April 1, 2002

RESPONSIBLE OFFICIAL(S):

Director, Office of Security Evaluation and Oversight

RECOMMENDATION #4:

The Chief, Information Technology Services, should ensure that the system operator command table for the SACS mainframes be modified to restrict user profiles to an appropriate level of access.

ASSESSMENT OF CAUSE:

The command code access was too liberal for certain profiles.

CORRECTIVE ACTION(S) TO RECOMMENDATION #4:

1a. The Office of Security Evaluation and Oversight (SEO) will assist Systems Support Division (SSD) in reviewing the table and in adjusting user profiles and established authorities. Specifically, SEO will distribute a memorandum to computing center management asking for review of the numbers and types of SACS user profiles and the command codes needed for the performance of each job.

1b. SEO will share the responses with SSD and coordinate establishment of appropriate user types and profiles.

1c. SEO will complete and submit SACS change requests, if necessary, for the actions to be taken.

1d. The Security Systems Software Section will provide the revised profiles for assignment by the Computing Centers.

1e. Computing Centers will assign the revised profiles to appropriate officials.

IMPLEMENTATION DATE(S):

1a. February 1, 2002

1b. March 1, 2002

1c. June 1, 2002

1d. July 1, 2002

1e. August 1, 2002

RECOMMENDATION #4 (cont'd):

RESPONSIBLE OFFICIAL(S):

1a. Director, Office of Security Evaluation and Oversight, M:S:S

1b. Director, Office of Security Evaluation and Oversight, M:S:S

1c. Director, Office of Security Evaluation and Oversight, M:S:S

1d. Chief, IBM Systems Software Branch, M:I:SS:IS

1e. Director, Enterprise Operations, M:I:E

LIMITED OFFICIAL USE

RECOMMENDATION #5:

The Chief, Information Technology Services, should ensure the Directors, TCC and System Support Division take action to ensure that all users with restricted systems programmer profiles on the SACS mainframes are brought into compliance with the SACS access standards or request approval from the Office of Security, Evaluation, and Oversight to deviate from the access standard for these users.

ASSESSMENT OF CAUSE:

The command code access was too liberal for certain profiles.

CORRECTIVE ACTION(S) TO RECOMMENDATION #5:

1a. The Office of Security Evaluation and Oversight (SEO) will assist Systems Support Division (SSD) in reviewing the table and in adjusting user profiles and established authorities. Specifically, SEO will distribute a memorandum to computing center management asking for review of the numbers and types of SACS user profiles and the command codes needed for the performance of each job.

1b. SEO will share the responses with SSD and coordinate establishment of appropriate user types and profiles.

1c. SEO will complete and submit SACS change requests, if necessary, for the actions to be taken.

1d. The Security Systems Software Section, of the Systems Software Branch, will provide the revised profiles for assignment by the Computing Centers.

1e. Computing Centers will assign the revised profiles to appropriate officials.

1f. SEO will issue interim guidelines, standards, and procedures.

IMPLEMENTATION DATE(S):

1a. February 1, 2002

1b. March 1, 2002

1c. June 1, 2002

RECOMMENDATION #5 (cont'd):

IMPLEMENTATION DATE(S) (cont'd):

1d. July 1, 2002

1e. August 1, 2002

1f. July 1, 2002

RESPONSIBLE OFFICIAL(S):

1a. Director, Office of Security Evaluation and Oversight, M:S:S

1b. Director, Office of Security Evaluation and Oversight, M:S:S

1c. Director, Office of Security Evaluation and Oversight, M:S:S

1d. Chief, IBM Systems Software Branch, M:I:SS:IS

1e. Director, Enterprise Operations, M:I:E

1f. Director, Office of Security Evaluation and Oversight, M:S:S

RECOMMENDATION #6:

The Chief, Information Technology Services, should revise the access control standard documentation for the SACS environment to include: new and/or updated information on the SACS operator commands; guidance to assist SACS security administrators in assigning appropriate SACS profile to users; and access standards for the SACS-related datasets on the IAP mainframes. These standards should also include a waiver process similar to ones in place for other IRS mainframe environments.

ASSESSMENT OF CAUSE:

SACS standard documentation has not been updated since its original release in 1994.

CORRECTIVE ACTION(S) TO RECOMMENDATION #6:

1a. The Office of Security Evaluation and Oversight (SEO) will assist the Security Systems Software Section, of the Systems Software Branch (SSB), in revising the access control standard documentation for the SACS environment. The documentation will reference the SACS-related datasets on IAP mainframes.

1b. The actual standards are included in the IAP Access Matrix maintained jointly by SSB and computing center security administrators.

1c. The issuance of SACS standards on console security will include a waiver process similar to that documented for use in other IRS systems. The documentation cannot be completed until all actions are taken on the system including those required for outstanding SACS change requests currently scheduled for completion by July 18, 2002.

IMPLEMENTATION DATE(S):

1a. July 1, 2002

1b. Completed – March 1, 2001

1c. July 1, 2002

RECOMMENDATION #6 (cont'd):

RESPONSIBLE OFFICIAL(S):

1a. Director, Office of Security Evaluation and Oversight, M:S:S

1b. Chief, IBM Systems Software Branch, M:I:SS:IS

1c. Director, Office of Security Evaluation and Oversight, M:S:S

RECOMMENDATION #7:

The Chief, Information Technology Services, should ensure the Directors, MCC and TCC take action to ensure that the SACS environment is compliant with the revised SACS access control standards once they have been prepared.

ASSESSMENT OF CAUSE:

Incomplete and outdated access standards for the SACS environment.

CORRECTIVE ACTION(S) TO RECOMMENDATION #7:

Action will be taken to ensure the SACS environment is compliant with the revised SACS access control standards once they are completed. This action is dependent upon issuance of SACS access control Guidelines, Standards, and Procedures (GSPs) by the Office of Security Evaluation and Oversight and their implementation.

IMPLEMENTATION DATE(S):

September 1, 2002

RESPONSIBLE OFFICIAL(S):

Director, Enterprise Operations

RECOMMENDATION #8:

The Chief, Information Technology Services should develop access standards for the Extended Operations Console Facility (EOCF) systems that specify guidelines and requirements for use by security personnel in administering the EOCF systems.

ASSESSMENT OF CAUSE:

Incomplete and outdated access standards for the SACS environment.

CORRECTIVE ACTION(S) TO RECOMMENDATION #8:

Office of Security Evaluation and Oversight (SEO) will assist the Security Systems Software Section, of the Systems Software Branch, in developing access standards and security administration documentation for the EOCF systems. The documentation will be provided to security administrators at computing centers.

IMPLEMENTATION DATE(S):

December 1, 2002

RESPONSIBLE OFFICIAL(S):

Director, Office of Security Evaluation and Oversight, M:S:S

RECOMMENDATION #9:

The Chief, Information Technology Services should reassign security administration responsibilities for the EOCF systems to an independent security function, such as the security functions in the MCC and TCC.

ASSESSMENT OF CAUSE:

Security Systems Software Section never migrated EOCF security to Computing Centers after CRS to SACS consolidation.

CORRECTIVE ACTION(S) TO RECOMMENDATION #9:

Security Systems Software Section, of the Systems Software Branch, will provide training and transfer security responsibilities for EOCF to the Computing Centers upon completion of pending MITS realignment.

IMPLEMENTATION DATE(S):

July 1, 2003

RESPONSIBLE OFFICIAL(S):

Chief, IBM Systems Software Branch, M:I:SS:IS

RECOMMENDATION #10:

The Chief, Information Technology Services should ensure that EOCF user access is annually re-certified and that audit trail reports on user activity are generated weekly and distributed to user management for review.

ASSESSMENT OF CAUSE:

EOCF re-certification was not occurring and no reporting mechanism was provided with the EOCF product.

CORRECTIVE ACTION(S) TO RECOMMENDATION #10:

1a. Actions were taken to address this weakness and re-certification was completed by the Systems Software Branch.

1b. The Office of Security Evaluation and Oversight will establish a task force to evaluate and review this weakness and propose a solution.

IMPLEMENTATION DATE(S):

1a. Completed – August 30, 2001

1b. September 1, 2002

RESPONSIBLE OFFICIAL(S):

1a. Chief, IBM Systems Software Branch, M:I:SS:IS

1b. Director, Office of Security Evaluation and Oversight, M:S:S