# The General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved

**August 1999**

**Reference Number: 199920063**

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

August 24, 1999

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved

This report presents the results of our review of the general controls over the Internal Revenue Service's (IRS) Unisys 2200 Operating System Environment. In summary, we found that the general controls over the operating system environment of the Unisys 2200 mainframe computers are adequately defined to protect sensitive data. However, we identified several areas in which controls could be adhered to more uniformly and where procedures should be established to provide improved system control, security, and standardization.

To improve controls over the system environment of the Unisys 2200 mainframes, we recommended several ways to improve controls over taxpayer data files, and common system and database files. In addition, we recommended modification of control settings for files that may potentially complicate the mainframe consolidation process. We also recommended a means to improve the accountability of individuals using the system security user-id, re-issuance of the policy for accounting for deviations of user access profiles from IRS standards, and development of C2-level security documentation, security policies, and documentation of risk factors for the Unisys consolidated mainframe environment.

IRS management agreed with the facts cited in the report and is taking appropriate corrective action. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as Appendix VII.

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 your staff may call Scott Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

# Table of Contents

# Executive Summary

The Internal Revenue Service's (IRS) Unisys 2200 mainframe computers are an integral part of its tax processing system. Virtually all transactions affecting a taxpayer's account are processed through these Unisys systems before being posted to the full taxpayer account on IRS' Masterfile database. The Unisys systems process tax returns that are sent to IRS' service centers by taxpayers. In addition, these systems house databases used by the Integrated Data Retrieval System for on-line retrieval of taxpayer information. The IRS will be migrating from a Unisys 2200 to a Unisys 4800 environment as part of the service center mainframe consolidation and will be operating under a more current version of the operating system.

The overall objective of the review was to determine whether general controls in place over the Unisys 2200 operating system are sufficient to protect sensitive data. The scope of this review encompassed system policies as they relate to security controls. We conducted our review in the IRS' National Office and on-site at the Andover (ANSC) and Austin (AUSC) Service Centers and the Martinsburg Computing Center (MCC). In addition, we reviewed system reports from the Cincinnati, Fresno, and Philadelphia Service Centers.

## Results

The general controls over the operating system environment of the Unisys 2200 mainframe computers are adequately defined to protect sensitive data. Specifically, each user is uniquely recognized and verified by the operating system. In addition, discretionary access controls (e.g., file ownership and access control records) are enforced through the security software residing on the mainframe computer. Access to most sensitive taxpayer data files, as well as any security-related actions, are monitored by management.

We identified several areas in which controls could be adhered to more uniformly and where procedures should be established to provide improved system control, security, and standardization. Memoranda dealing with site-specific control weaknesses have been issued to the responsible local officials. This report addresses systemic issues that require corrective actions throughout the IRS.

Although the Unisys 2200 mainframe computers will become obsolete due to the IRS' mainframe consolidation efforts, steps need to be taken now to better prepare the Unisys 2200 systems for consolidation. In addition, due to the similarities in the operating systems of both systems, control improvements identified on the Unisys 2200 systems should also be implemented on the Unisys 4800 systems to improve its control environment.

## Access to Sensitive Taxpayer Data Files by System Users Is Not Always Reported to Management

Over 6,200 files at the 5 service centers are established in a way that permits any system user to view their contents. From a judgmentally selected sample of 109 such files at the ANSC and AUSC, we identified 10 files that contained taxpayer data. Since these files are not properly recorded on the system, accesses to them are not recorded on weekly reports used by management to monitor access to taxpayer data by system users.

## Access Control Settings Are Not Consistent among Some Common System Files

Over 10 percent of the files common to the Unisys production environment at 4 service centers contain inconsistencies in access control settings, such as file ownership and clearance (security) levels. The inconsistencies appear to be an unintentional side effect of actions taken to recover files or solve system problems. These inconsistencies may cause problems in the Unisys 4800 consolidated environment. The Office of Management and Budget (OMB) suggests that part of a consolidation strategy should be the development of a plan to optimize data center operations, which would be achieved in part through standardization of the operating system.

## Many Cataloged Files Have No Owner Designated or Are Not Owned by Current System Users

Over 1,200 files at 5 service centers were either recorded without an assigned owner or assigned to a user-identification (user-id) that was no longer active on the system. Files with incorrect ownership assignments can cause problems during the consolidation from the Unisys 2200 to the Unisys 4800 environment. MCC personnel informed us that problems arose in moving improperly owned files during the mock move between the Brookhaven Service Center and MCC. Although a temporary solution was found for the actual conversion, the solution left the IRS with the continued existence of improperly owned files. Internal Revenue Manual (IRM) guidelines do not address the need to reassign ownership for the files meeting these two conditions.

## Use of the System MASTER Account Is Not Traced to Individual System Users

In the current Unisys 2200 environment, there is no mechanism available to account for individual use of the MASTER user-id for the system. The MASTER user-id on the Unisys 2200 is one of the most powerful user-ids on the system, enabling its user to access all areas of the system. Although the MASTER user-id was used primarily by the security analysts at ANSC and AUSC as their sole user-id, several other users also had access to the password in emergency situations. The IRM requires that the system security officer or systems administrator be able to selectively audit the actions of one or

more users based on individual identity. These audits should include all actions of the MASTER user-id.

## The User Profile Deviation Process Has Not Been Working as Intended

Our review of deviation forms used to request modifications to standard Unisys 2200 user profiles indicated that a number of profile changes made by the service center personnel had not been reviewed or signed by the responsible IRS National Office functions. These omissions were due in part to required IRS National Office functions not receiving the deviation forms for review. The IRS' Unisys 2200 Access Standards require completion and approval of a deviation form when changes to the standard profiles are needed for system users to perform their duties. Since the security system of the Unisys 2200 system is very complex, modifications made without proper review and approval can have unforeseen serious consequences.

## Several Treasury and Office of Management and Budget Requirements for Automated Information Systems Have Not Been Met on the Unisys 2200 Mainframes

Department of Treasury directives require that all Treasury automated information systems transmitting sensitive but unclassified information meet a C2 level of protection (see Appendix V). The IRS' Unisys 2200 systems are operating in a non-C2 compliant environment and without an approved waiver of compliance. In addition, we were unable to locate documentation for the testing of the system's security features.

The OMB requires that controls over general support systems include a system security plan. The OMB also requires that Federal agencies determine the adequacy of their systems' security, which may be conducted using a risk-based approach. We were unable to locate documentation of risk factors or a security plan for the Unisys 2200 systems.

# Summary of Recommendations

- All files with taxpayer information that are readable by the casual system user should be identified and immediately secured.
- Control settings for files common to the Unisys 2200 production mainframes should be standardized.
- Prior to migration to the consolidated environment, all improperly owned files should be identified and assigned to an active system user. For future user-id removals, a policy should be instituted requiring that all files owned by such users be deleted or assigned to an active system user.

- Information Systems should examine and implement, if feasible, the ability to track individual actions of users accessing the MASTER user-id on the Unisys 4800 system.
- The policy for submitting profile deviation forms to the IRS National Office should be formally re-issued and all unapproved deviation forms should be submitted to all required IRS National Office functions for review and approval.
- All required C2 documentation, security policies, and risk factor documentation should be prepared for the Unisys 4800 environment.

Management's Response: IRS management agreed with the facts cited in the report and is taking appropriate corrective action. Management's comments are included in the body of the report, where appropriate, and a complete text appears as Appendix VII.

## Objective and Scope

This report presents the results of our review of the general control environment[1] over the Internal Revenue Service's (IRS) Unisys 2200 operating system. Our work was conducted in accordance with *Government Auditing Standards* from July to December 1998. We conducted our review in the IRS' National Office and on-site at the Andover (ANSC) and Austin (AUSC) Service Centers and the Martinsburg Computing Center (MCC). In addition, we reviewed system reports from the Cincinnati (CSC), Fresno (FSC), and Philadelphia (PSC) Service Centers.

The overall objective of this review was to determine whether general controls in place over the Unisys 2200 operating system are sufficient to protect sensitive data. In addition, we compared system parameters and control settings across the five service centers. The scope of this review encompassed system policies as they relate to security controls.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

## Background

The IRS' Unisys 2200 mainframe computers are an integral part of the agency's tax processing system. Virtually all transactions affecting a taxpayer's account are processed through these Unisys systems[2] before being posted to the full taxpayer account on IRS'

[1] In this report, the term "environment" will be used to refer to all IRS systems of a particular configuration (e.g., Unisys 2200 or 4800).

[2] In this report, the term "system" will be used to refer to the hardware and operating system software of a Unisys mainframe computer.

Masterfile database. The Unisys systems process tax returns that are sent to IRS' service centers by taxpayers. In addition, these systems house databases used by the Integrated Data Retrieval System for on-line retrieval of taxpayer information.

Currently, the IRS is in the process of consolidating the mainframe operations of the 10 service centers into the 2 computing centers in Martinsburg, West Virginia, and Memphis, Tennessee. As part of its consolidation efforts, the IRS will be migrating to a Unisys 4800 environment that will operate under a more current version of the operating system. The Unisys phase of mainframe consolidation will be completed over a three-year period. As of the end of 1998, Unisys mainframe processing at three service centers was migrated to the consolidated environment. At the time of our review, four more service centers were planned to be consolidated in 1999, with the remaining three systems to be consolidated in 2000.

There was an average of 120 system-level users on each of the 5 service center systems at the time of our review. Security and identification of these users is administered through the Site Management Complex (SIMAN). User access is controlled through user-identifications (user-ids), passwords, clearance levels, and control over access privileges. Clearance levels are a 64-level hierarchical security classification system for users and files, ranging from 0 (zero), the lowest, to 63, the highest level of security.

SIMAN is also used to administer access controls over cataloged files, which is achieved through both mandatory and discretionary access controls. Cataloged files are files that are recorded on the system's master directory. Mandatory controls include clearance levels and access privileges. Discretionary controls include file ownership and access control records (ACR). File owners are responsible for the content of their files. ACRs contain a list of users, the accesses granted to a given file, and the conditions under which the users are allowed access. Files not assigned an ACR are designated as either PUBLIC, making them accessible

by any system user, or PRIVATE, which permits access by the file owner only.

## Results

*The general controls over the operating system of the Unisys 2200 mainframes are adequately defined to protect sensitive data.*

The general controls over the operating system of the Unisys 2200 mainframes are adequately defined to protect sensitive data. Specifically, each user is uniquely identified and authenticated by the operating system. In addition, discretionary access controls are enforced through the SIMAN security software residing on the mainframe. Access to most sensitive taxpayer data files, as well as any security-related actions, is monitored by management.

*We identified several areas in which controls should be adhered to more uniformly and where procedures should be established to provide improved system control, security, and standardization.*

We identified several areas in which controls should be adhered to more uniformly and where procedures should be established to provide improved system control, security, and standardization. Memoranda dealing with site-specific control weaknesses have been issued to the responsible local officials. This report addresses the following systemic issues that require corrective action throughout the IRS:

- Access to sensitive taxpayer data files by system users is not always reported to management.
- Access control settings are not consistent among some common system files.
- Many cataloged files have no owner designated or are not owned by current system users.
- Use of the system MASTER account is not traced to individual system users.
- The user profile deviation process has not been working as intended.
- Several Treasury and Office of Management and Budget (OMB) requirements for Automated Information Systems have not been met on the Unisys 2200 mainframes.

In support of this review, we requested from the Office of Security Standards and Evaluation (SSE) a listing of findings they identified during their security reviews of Unisys systems at IRS service centers. We requested information regarding the findings, their status, and the dates of the findings and any corrective actions. Personnel in the Office of SSE provided us with a listing of only their findings in July 1998. Repeated attempts to obtain all of the requested information before our on-site visits to the ANSC and AUSC were unsuccessful. Consequently, we were not able to complete a portion of our audit program while on-site. After discussing the request with the Office of SSE in October 1998, we were eventually provided the information, but it was too late to perform our on-site tests.

## Access to Sensitive Taxpayer Data Files by System Users Is Not Always Reported to Management

*Accesses to some files containing taxpayer data would not be contained in Live Data Reports sent to management at ANSC and AUSC.*

We determined that accesses to a number of files with taxpayer data would not be included in reports used by management to monitor such access. We reviewed access controls for the cataloged files on the five service center Unisys 2200 systems. We identified a large number of files on each system that were cataloged at the lowest clearance level (zero) and were designated such that any system user could view them (PUBLIC). This PUBLIC designation is only permissible for files not secured by an ACR.

Files with these access control settings are readable by any system user, with such access not reported to management. The number of this type of file for each center is shown in Table 1.

| Service Center | Number of Clearance Level 0, PUBLIC files |
|---|---|
| ANSC | 1,081 |
| AUSC | 1,157 |
| CSC | 842 |
| FSC | 1,740 |
| PSC | 1,386 |
| **Total** | **6,206** |

*Table 1: Number of files that can be accessed without being reported to management*

We judgmentally reviewed samples of these types of files at AUSC and ANSC. We also judgmentally selected several additional files that were cataloged at a clearance level of zero and were assigned the production user-id (PROD) ACR in order to determine the readability of these files. Of the 109 files sampled, we identified 10 files that contained sensitive taxpayer information, such as names, addresses, and taxpayer identification numbers.

*Some files containing taxpayer data are not cataloged at the proper clearance level.*

Access to the 10 files was not reported to management since the files were incorrectly cataloged at a clearance level of zero instead of the proper clearance level 31. Appendix IV contains further information on clearance levels. Access to files cataloged at clearance level 31 is recorded on a Live Data Access Report, which is reviewed by management weekly. Since accesses to these files were not included in the Live Data Access Report sent to management, any access of taxpayer data in the files was not monitored.

The Information Systems Operations and Management section of the Internal Revenue Manual (IRM) states that a primary responsibility of the IRS is to safeguard the integrity of taxpayer data maintained in its computer files. In addition, because of the importance of protecting taxpayer data, the IRS must continue to strengthen the methods of controlling and documenting access to computerized taxpayer data files.

## Recommendations

1. The Chief Information Officer should ensure that the 10 files we identified with taxpayer information are immediately secured to prevent system users from casually reviewing the taxpayer data contained in the files without such access being reported to management.

Management's Response: Management agreed to review the 10 files and their relationship with other production files to determine whether it is feasible to secure the files without disrupting production activity at ANSC and AUSC. If, after reviewing the files, it is determined that production will not be disrupted, management will determine the appropriate actions to be taken and develop an action plan accordingly.

2. The Chief Information Officer should ensure all system files cataloged at clearance levels other than 31 that are readable by the casual system user are reviewed for the existence of taxpayer data. If identified, the files should be protected to ensure that casual accesses to files are either prevented or reported to management.

Management's Response: Based on analysis of the 10 files in Recommendation #1, management will determine the ownership of any file below clearance level 31 and request the file owner to provide the sensitivity of the file.

## Access Control Settings Are Not Consistent among Some Common System Files

*Access control settings are not consistent for a number of files common to the IRS' Unisys 2200 production environment.*

Our review of the access control settings over cataloged files on the Unisys 2200 mainframes also identified numerous differences in the access control settings for some of the files. We excluded PSC from this analysis since a large number of files had been purged from its system, as a part of their routine maintenance, at the time the reports for our audit were generated. There were over 4,800 files common to each of the 4

mainframes reviewed, comprised of significant numbers of common, IRS-wide cataloged files. Analysis of these common files identified inconsistencies in access control settings for 11 to 13 percent of the files reviewed, depending on the control setting. The control settings reviewed and the results of review are shown in Table 2. Of the files identified in Table 2, there were 212 common files with inconsistent settings for all 3 access controls reviewed.

*Access controls include file ownership, clearance levels, and access control records.*

| Access Control | Number of Files with Inconsistent Control Settings | Percentage of Common Files |
|---|---|---|
| File Owner | 529 | 10.9% |
| Clearance Levels | 586 | 12.1% |
| Access Control Records | 632 | 13.1% |

*Table 2: Review of inconsistent file control settings*

*Inconsistencies in control settings may be an unintentional side effect of actions taken to recover files or solve system problems.*

IRS National Office Information Systems (IS) personnel informed us that these differences might be an unintentional side effect of actions taken to recover files or solve system problems. Personnel taking these actions, typically database administrators (DBA) or computer systems analysts, at times, may do so without regard for the proper control settings of the file, such as when problems arise in emergency situations that must be corrected quickly. This problem can be illustrated by the following example:

> A DBA may work on a file that is cataloged at a clearance level of 31 and owned by the user-id PROD. After work is completed, the DBA might catalog the file again, but do so at a lower clearance level, such as 0. This setting will remain in effect until the DBA or Security Analyst changes it to the proper setting.

We also identified 130 files cataloged at clearance levels other than the 4 levels specified by the IRS National Office. These specified clearance levels are 0, 30, 31, and 63, and are further defined in Appendix IV. A majority of the files cataloged at the unspecified clearance levels are used in the program transmittal system, which is used to transmit authorized computer

programs and changes to them into production. These files are broken out by service center and clearance level in Table 5 of Appendix IV.

IRS National Office IS personnel informed us that the service centers are given discretion in cataloging files at clearance levels other than those specified by the IRS National Office. There are no procedures in place to notify necessary IRS National Office personnel of the use of these discretionary clearance levels.

*Users needing to access the same file for different service centers on the Unisys 4800 system may run into problems if control settings are not consistent on a given file.*

Both inconsistent control settings and the use of unspecified clearance levels for common files could cause problems in the consolidated Unisys 4800 environment. Due to the technology used by the Unisys 4800 system, users needing to access the same file for different service centers may experience problems if permissions are not consistent on a given file. This occurs especially if the inconsistent setting is outside the range of privileges for a given user's profile. In addition, updates to the same files for multiple service centers may increase the work needed to maintain the system.

The OMB calls for agencies to reduce the number of agency data centers as well as the total cost of data center operations. The OMB suggests that part of a consolidation strategy should be the development of a plan to optimize data center operations, which can be achieved in part through standardization of operating systems. A uniform system of file access control settings would assist in standardizing the Unisys operating system.

## Recommendation

3. The Chief Information Officer should standardize control settings for files common to the Unisys 2200 production mainframes. Such a process should begin with the identification of files common to the Unisys 2200 production systems and a determination of the standard security attributes for each.

Management's Response: Standardized control settings for files common to the Unisys 2200 production mainframes will be established pending identification of files common to the Unisys 2200 mainframes by IS in coordination with other IRS organizations.

## Many Cataloged Files Have No Owner Designated or Are Not Owned by Current System Users

*All five systems reviewed contained both unowned files and files owned by user-ids that had been previously removed from the system.*

Each of the five Unisys 2200 mainframes reviewed contained unowned files, as well as files that were owned by user-ids that had been previously removed from the system. The number and type of improperly owned files, by service center, are identified in Table 3.

| Issue | Service Center | | | | |
|---|---|---|---|---|---|
| | ANSC | AUSC | CSC | FSC | PSC |
| Unowned Files | 14 | 95 | 114 | 107 | 3 |
| Files Without Current Owners | 112 | 117 | 136 | 263 | 298 |

*Table 3: Number of improperly owned files identified on five service center Unisys 2200 systems*

Under the SIMAN security package, unowned files can be created only if a special parameter is set for a given user. However, owners can also be removed from cataloged files using the SIMAN. We were informed that there are some legitimate reasons for files not to have owners. For example, an owner may be removed when files need to have keys set for read or write access, such as for production transmittal files.

*IRM guidelines do not contain requirements for re-assignment of file ownership after a user's removal from the system.*

The existence of files owned by user-ids that were no longer present on the system is often caused by the failure to reassign files after their owners have been removed from the system. The IRM sections on Automated Information Systems Security and Information Systems Operations and Management do

not include a policy requiring that files be removed or reassigned when a user is removed from the system.

These improperly owned files, especially those owned by users not present on the system, can cause problems during the IRS' mainframe consolidation efforts. The following example illustrates this type of problem:

> When an improperly owned file is moved to a Unisys 4800 mainframe, the system first compares the file owner to the system file of users for the mainframe. If the owner is not present in the user file, the file being moved is designated PRIVATE, so that only the system can access it. Subsequent moves of any remaining cycles of the same file can create problems since the control settings of the cycle being moved do not match those of the initial cycle. These subsequent cycles are not moved to the consolidated system and are consequently dropped.

*Problems with files owned by non-current user-ids were encountered during the mock move of the Brookhaven Service Center.*

MCC personnel indicated that problems such as this were identified in over 1,400 files during the mock move from the Brookhaven Service Center to the MCC. Through the use of dummy user-ids, IRS personnel were able to successfully move the improperly owned files. However, this solution only transferred the ownership problem while at the same time creating an entirely new problem. Improperly owned files moved to MCC remained improperly owned since the dummy user-ids used in the transfer were deleted after the move. In addition, the removal of dummy user-ids leaves behind ACRs that must eventually be rewritten, since ACRs cannot be deleted from the system.

## Recommendations

4. The Chief Information Officer should ensure all improperly owned files are identified and assigned an owner present on the Unisys 2200 system at each service center, with the exception of files required to be unowned, prior to movement of that service center's mainframe to the consolidated Unisys 4800 environment.

Management' Response: Management is working to identify improperly owned files and will develop a process to modify the profile of improperly owned files prior to the consolidation of a particular service center.

Management will also review each service center's Unisys 2200 files for improper ownership both throughout the consolidation process and during their regularly scheduled reviews at the service centers.

5. The Chief Information Officer should institute a policy requiring that all files owned by users being removed from the Unisys 2200 and Unisys 4800 systems either be deleted or assigned to a user present on the system.

Management's Response: Management will develop guidelines to address file ownership in the Unisys mainframe environment. Implementation of the guidelines will require a technical solution that will be incorporated into the IRM when completed. When the guidelines are completed, management will implement them at the service centers that, at the time, have not been consolidated. The guidelines will also be implemented at the MCC and Tennessee Computing Center.

## Use of the System MASTER Account Is Not Traced to Individual System Users

*The Unisys 2200 system does not possess a mechanism to monitor each user accessing the MASTER user-id.*

The MASTER user-id on the Unisys 2200 system is one of the most powerful user-ids on the system, enabling its user to access all areas of the system. Currently, the security analyst for each system we reviewed on-site uses MASTER as their sole user-id. However, several other users, such as the backup security analyst and data security chief, also have access to the password for the MASTER user-id in emergency situations. Security personnel at the sites we visited informed us that the MASTER password is changed each time it is accessed by one of the other authorized users. Any security actions initiated by MASTER, or any other user-id, are recorded on a security actions report generated at the service centers.

IRS National Office personnel informed us that use of the MASTER user-id on the operating system of the

Unisys 2200 systems cannot be traced back to individual users. However, they also informed us that the operating system of the Unisys 4800 has overcome this limitation, although the operating effects of this feature are unclear at this time.

The IRM requires that the system security officer or systems administrator shall be able to selectively audit the actions of one or more users based on individual identity. These audits should include the actions of both the corporate use of the MASTER user-id as well as the individual users accessing the MASTER user-id.

### Recommendation

6. The Chief Information Officer should examine the possibility of tracking individual user actions while using the MASTER user-id on the Unisys 4800 system and, if possible, implement this feature as soon as feasible.

Management's Response: Management will review the possibility of relating the use of the MASTER user-id to a specific human user. In addition, as service centers are consolidated, management will better define procedures on the use of the sub-system administrator option in the Unisys 4800 environment.

## The User Profile Deviation Process Has Not Been Working as Intended

*Not all required signatures were present on user profile deviation forms at AUSC.*

Our review of the forms used to request modifications to standard Unisys 2200 system user profiles revealed that not all required signatures were present. At AUSC, personnel had approved these deviation forms; however, there was no evidence that they had been reviewed or signed by any of the required IRS National Office functions. Some of these forms were initiated as far back as January 1997. Discussions with IRS National Office personnel also revealed that deviation forms had not been received by some of the specified functions.

User access to the Unisys 2200 system is governed by a set of Unisys Access Standards maintained by the Office of SSE. These standards provide for exceptions to standard user profiles, as conditions warrant, through submission of profile deviation forms. These deviation forms are approved by service center management and reviewed by several IRS National Office functions.

The Unisys Access Standards were issued in March 1996 and revised in July 1996. Since then, the IS function has been reorganized several times, resulting in the reassignment of functional responsibilities and the creation and consolidation of functions within the organization. Consequently, some of the IRS National Office organizations specified in the Unisys Access Standards no longer exist.

*Without proper approval of user profile deviations, modifications may be made with unforeseen consequences.*

Modifications made to user profiles without proper review and approval can have unforeseen serious consequences. The security system of the Unisys 2200 operating system is complex, with numerous features provided for file and user security. If IRS does not review the impact of user profile modifications on other profile security features, then possible security exposures may not be identified. One such exposure is the declassification of data that can result when a user is granted certain privileged interfaces. The following example further illustrates this complexity:

> It is dangerous in systems without transaction processing (TIP) file security to grant a user access to privileged interfaces FCREG$ and PB$CON. The combination of these two privileged interfaces gives the user the ability to declassify data residing in an Exec file. Currently, the IRS' Unisys 2200 systems are operating without TIP file security.

Problems in the deviation process were discussed with SSE personnel who informed us that the process is now working properly. Personnel in the Office of SSE informed us that they sent several electronic mail (e-mail) messages to all Unisys security analysts revising the deviation process last year. Prior to these e-mail messages, the Office of SSE had not been receiving all of the deviation forms. The Office of SSE assured us

that, after issuance of the e-mail messages, the deviation forms were properly routed.

### Recommendations

7. The Office of SSE management should issue a memorandum to all Unisys security analysts formally outlining the revised Unisys Access Standards deviation process.

Management's Response: Management formally issued a memorandum to the service and computing centers on October 7, 1998, requiring that any deviation be documented and submitted to the IRS National Office for review and approval.

8. The Chief Information Officer should ensure that all unapproved deviation forms are submitted to all required IRS National Office functions for review and approval.

Management's Response: Management is continually working to ensure that any deviation from the current Unisys 2200 Access Standards is documented and submitted to the IRS National Office for review and approval/disapproval.

## Several Treasury and Office of Management and Budget Requirements for Automated Information Systems Have Not Been Met on the Unisys 2200 Mainframes

*An approved waiver of C2 compliance for the Unisys 2200 could not be located.*

The IRS' Unisys 2200 systems are operating in a non-C2 compliant environment and without an approved waiver of compliance. Although field personnel informed us that a waiver of C2 requirements existed, we were able to locate only an unapproved draft C2 waiver for the Unisys 2200 system. Appendix V provides a brief description of C2 requirements.

*There is no security policy for the Unisys 2200 or C2 required test documentation.*

During our on-site visits, we reviewed various security documents for the Unisys 2200 systems provided by field personnel. The sites maintained most of the documents required for C2 compliance. We were

provided copies of a Security Features User's Guide, Trusted Facility Manual, and system design documentation for the Unisys 2200 systems we reviewed on-site (ANSC and AUSC). However, documentation for the testing of the systems' security features was not available. We were also informed while on-site that a security policy for the Unisys 2200 environment did not exist.

While on-site, we also asked whether a risk assessment had been performed on the Unisys 2200 environment. We were informed that no such assessment had been conducted specifically for the Unisys 2200. In addition, we were informed that no documentation exists of an IRS-wide assessment of any risk management factors for the Unisys 2200 environment.

Treasury Directives require that all Treasury automated information systems that transmit sensitive but unclassified information meet a C2 level of protection. In addition, the OMB requires that agencies plan for the adequacy of system security, which should be conducted using a risk-based approach. This approach includes consideration of risk factors such as the value of the system, as well as threats, vulnerabilities, and effectiveness of current or proposed safeguards. The OMB also requires that all agencies shall implement and maintain a security program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. This program should include a system security plan.

Since the Unisys 2200 mainframes will be phased out and eventually replaced, the preparation of C2 documentation and a formal risk assessment for the Unisys 2200 may not be the best use of scarce IS resources. However, every attempt should be made to achieve C2 compliance and assess risk factors of, and develop a security plan for, the Unisys 4800 system.

### Recommendations

9. The Chief Information Officer should ensure that all required C2 documentation is prepared for the Unisys 4800.

10. The Chief Information Officer should develop and maintain a security policy for the Unisys 4800.

11. The Chief Information Officer should conduct and document an assessment of the risk factors for the Unisys 4800.

Management's Response: A task order has been issued with a contractor on the Service Center Mainframe Consolidation project to develop C2 documentation, security policies, and documentation of risk factors. Management is also working with the contractors to ensure that the documentation is developed and tested for the consolidated mainframe environment. Management will develop and maintain an IRS Security policy for the Unisys 4800 in conjunction with the task order.

## Conclusion

Although the Unisys 2200 mainframes will become obsolete due to the IRS' mainframe consolidation efforts, steps need to be taken now to better prepare the Unisys 2200 systems for consolidation. In addition, due to the similarities in the operating system of both environments, control improvements identified for the Unisys 2200 systems should also be implemented on the Unisys 4800 systems to improve its control environment.

**Appendix I**

## Detailed Objective, Scope, and Methodology

The overall objective of the review was to determine whether general controls in place over the Unisys 2200 operating system are sufficient to protect sensitive data. The scope of this review encompassed the review of system policies as they relate to security controls. In addition, identification and authentication controls, discretionary access controls, system (as opposed to the Integrated Data Retrieval System) audit trail policies, and disaster recovery and database back-up policies were reviewed. Specifically, we:

I. Obtained background information to gain an understanding of the system.

A. Reviewed Office of Management and Budget (OMB) requirements, specifically:

- OMB Circular A-130 Appendix III.
- OMB Bulletin 96-02.

B. Reviewed Treasury Directive P 71-10, Treasury Information Security Manual.

C. Reviewed Internal Revenue Manual (IRM) Sections on Information Systems (IS), specifically:

- IRM 2700: Information Systems Operations and Management.
- IRM 2(10)00: Automated Information Systems Security.

D. Reviewed the Unisys 2200 Access Standards, including sections on profile deviation reporting.

E. Reviewed Unisys 2200 system documentation, including:

- Unisys 2200 Security Planning and Administration Guide.
- Unisys 2200 Site Management Complex Administration and End Use Guide.
- Exec System Software Installation and Configuration Guide.

II. Reviewed the overall Unisys security policies at the visited sites.

A. Determined if periodic risk assessments were performed.

B. Reviewed the completeness of the security program plan and the frequency with which it is updated.

C. Reviewed the adequacy of the security management structure over the system.

D. Reviewed the adequacy of security-related personnel policies.

E. Determined whether management was monitoring the security program's effectiveness.

F. Obtained a list of all users on the system and determined what procedures were used to verify that they still need system access.

G. Determined who had system administrator privileges and how this privilege was restricted.

III. Assessed the adequacy of system access controls.

A. Identified controls in place over the system's user accounts and evaluated the adequacy of these controls for preventing unauthorized individuals from accessing the system.

B. Evaluated usage of and control over privileged user accounts, files and utilities.

C. Reviewed user password settings and policies and evaluated their appropriateness.

D. Determined what library access controls were in place and evaluated the adequacy of these controls for restricting system and data file access to only appropriate individuals.

E. Determined if Unisys had provided operating system source code to the Internal Revenue Service, and if so, assessed the controls in place to ensure the code was only accessed by authorized individuals.

IV. Assessed controls over network or dial-up connections.

A. Observed the locations of all modems connected to the system. Evaluated the controls over the use of each of these modems.

B. Determined what type of network access the system supports and considered tests based on this level of access.

C. Evaluated the adequacy of procedures for controlling access through dial-in lines. Ascertained that the login process provided adequate controls to prevent unauthorized access. Also, determined whether an inventory of users who were authorized to access the system through these lines was documented.

D. Determined if data was transported through telecommunication lines and assessed security controls.

V. Assessed the system's ability to log auditable events and evaluated the adequacy of current recording and reviewing policies for detecting problems with accounts, file access, or remote connections at the system level.

A. Determined the availability of system audit trail data.

B. Reviewed the system audit trail logs to identify any employees who were logging on and not logging off, all after-hours access, etc.

C. Attempted to access files to which users did not have access based on the permissions information obtained in the previous step. Determined whether the access violation was recorded on the audit trail by viewing the audit log.

D. Ensured that the system administrator did not use his or her administrative account for tasks not requiring such access.

E. Determined whether system audit logs were reviewed, determined how often they were reviewed and by whom, and identified follow-up activities to violations.

VI. Assessed adequacy of controls in place to ensure service continuity in the event system operation is disrupted.

A. Determined whether database back-up and recovery procedures have been developed, implemented, and tested and assessed the adequacy of the procedures. (These procedures are generally developed to deal with unexpected system failures.)

B. Determined whether disaster recovery procedures have been developed, implemented, and tested and assessed the adequacy of the procedures. (These procedures are developed to deal with natural disasters.)

VII. Assessed the physical controls in place at the selected sites.

A. Conducted a walk-through of the computer room.

B. Observed physical security controls over the computer room and assessed their adequacy.

C. Observed physical security over user and developer terminals.

D. Assessed controls over tape/media library.

VIII. Assessed the effectiveness of corrective actions to recommendations made by the IS Office of Security Standards and Evaluation and determined whether they have been implemented.

IX. Determined the baseline for operation of the Unisys 2200.

A. Compared the configuration parameters for each of the service center Unisys 2200's reviewed and identified any differences.

B. Compared the service center baseline with the Martinsburg Computing Center Program Development System configuration parameters and identified any differences.

C. Compared the attributes of files common to all service center Unisys 2200's reviewed and identified any differences.

**Appendix II**

## Major Contributors to This Report

Scott Wilson, Associate Inspector General for Audit (Information Systems Programs)

Mike Phillips, Director

Vincent Dell'Orto, Audit Manager

Kent Sagara, Audit Manager

Mike Howard, Senior Auditor

Tony Hubbard, Senior Auditor

Jill Moore, Senior Auditor

**Appendix III**

## Report Distribution List

Deputy Commissioner Modernization C:DM

Deputy Commissioner Operations C:DO

Chief Information Officer IS

Deputy Chief Information Officer, Operations IS

Deputy Chief Information Officer, Systems IS

Assistant Commissioner National Operations IS:O

Assistant Commissioner Program Evaluation and Risk Analysis M:OP

Assistant Commissioner Service Center Operations IS:SC

Assistant Commissioner Systems Development IS:S

Director, Systems Standards and Evaluation IS:E

Director, Martinsburg Computing Center IS:O:M

Director, Security Standards and Evaluation IS:E:S

Director, System Support Division IS:S:SS

Director, Telecommunications and Operations Division IS:O:O

National Director for Legislative Affairs CL:LA

Office of Management Controls M:CFO:A:M

Audit Liaison (Attn: Frank Guarino) IS:I:IS:O:A

**Appendix IV**

## Details on Discretionary Clearance Levels

The Internal Revenue Service's (IRS) National Office has specified four clearance levels to be used for cataloging files on the Unisys 2200. These specified clearance levels are listed in Table 4.

| Class of files | Types of Files Included | Clearance Level |
|---|---|---|
| System Files | Production and operating system files | 0 |
| Development | Programming files | 30 |
| Live Data | Taxpayer data files | 31 |
| Security | Security-related system files | 63 |

*Table 4: National clearance level specifications*

We identified 130 files cataloged at clearance levels other than those specified by the IRS' National Office. A majority of these files are used in the program transmittal system, which is used to transmit authorized computer programs and changes to them into production. These 130 files are broken out by service center and clearance level in Table 5.

| Clearance Level | Andover | Austin | Cincinnati | Fresno | Philadelphia | Total |
|---|---|---|---|---|---|---|
| 1 | 15 | 14 | 14 | 27 | 26 | 96 |
| 3 | 0 | 0 | 0 | 0 | 2 | 2 |
| 5 | 0 | 1 | 0 | 0 | 0 | 1 |
| 8 | 0 | 0 | 13 | 0 | 0 | 13 |
| 10 | 0 | 0 | 9 | 0 | 0 | 9 |
| 21 | 0 | 0 | 0 | 0 | 1 | 1 |
| 62 | 4 | 0 | 0 | 0 | 4 | 8 |
| **Total** | **19** | **15** | **36** | **27** | **33** | **130** |

*Table 5: Discretionary file clearance levels in use at five service centers*

**Appendix V**

## Description of C2 Level Security

The Department of Defense has developed a multi-level system for classifying computer system security, commonly known as the Orange Book. The classification system ranges from class D (Minimal Protection) to class A1 (Verified Protection). The Department of the Treasury requires that its automated information systems "processing, storing, or transmitting sensitive but unclassified data will meet the requirements for a C2 level of protection (Controlled Access Protection)."

Systems in the C2 class enforce a finely grained discretionary access control mechanism, making users individually accountable for their actions. This accountability is achieved through login procedures, auditing of security-relevant events, and resource isolation. Systems in this class are required to achieve a minimum level of assurance through meeting requirements for system architecture, system integrity, and security testing. Federal agencies operating Class C2 systems are also required to maintain documentation covering the security features of the system as well as testing and design documentation.

The risk of not meeting one or more of the C2 level requirements can lead to the opening of security exposures in the system. For example, if a system does not meet the Object Reuse requirement (resource isolation), it runs the risk of having deleted data retrieved without the owner's consent. The Object Reuse section requires that the system assure that a storage object (e.g., disk file, etc.) has been cleared before it is initially assigned, allocated, or reallocated to a system user. Failure to clear the object before assignment allows the newly assigned user the opportunity to retrieve deleted data from the object.

**Appendix VI**

## Abbreviations Used In This Report

| Abbreviations | Term |
|---|---|
| ACR | Access Control Record |
| ANSC | Andover Service Center |
| AUSC | Austin Service Center |
| CSC | Cincinnati Service Center |
| DBA | Database Administrator |
| FSC | Fresno Service Center |
| IS | Information Systems |
| IDRS | Integrated Data Retrieval System |
| IRM | Internal Revenue Manual |
| IRS | Internal Revenue Service |
| MCC | Martinsburg Computing Center |
| OMB | Office of Management and Budget |
| PSC | Philadelphia Service Center |
| SIMAN | Site Management Complex |
| SSE | Office of Security Standards and Evaluation |
| TCC | Tennessee Computing Center |
| TIP | Transaction Processing |

## Appendix VII

## Management's Response to the Draft Report

COMMISSIONER

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

July 15, 1999

OFFICE OF TREASURY
INSPECTOR GENERAL
RECEIVED
TCMS
1999 JUL 19 A 9:37
199907-49VHBXCN
FOR TAX ADMINISTRATION

MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Management Response to Draft Audit Report - the General Controls Environment Over the Internal Revenue Service's Unisys 2200 System Can Be Improved

The Information Systems (IS) organization has completed its review of the subject Draft Audit Report. The management response is attached.

The consolidation of mainframe tax processing computers from ten service centers to two computing centers is one of the IRS' major initiatives. I chair a monthly Executive Steering Committee with representatives from Treasury, the IRS, and the National Treasury Employees Union which monitors key risks to ensure that all necessary actions are being taken.

While the current Unisys 2200 mainframe computers will become obsolete due to the IRS' mainframe consolidation efforts, IS is taking actions to better secure the Unisys 2200 system controls prior to consolidation. In addition, due to the similarities in the operating systems of the Unisys 2200 and the Unisys 4800, IS is implementing control improvements identified for the Unisys 2200 systems on the Unisys 4800 systems to improve their control environment.

Specifically, the Assistant Commissioner for IS National Operations, the Assistant Commissioner for Systems Development, and the Director, Office of Systems Standards and Evaluation, are addressing the issues raised in this audit regarding security of taxpayer information. This effort will result in policies and guidelines which will also be implemented for the Unisys 4800 environment under mainframe consolidation. In addition, IS is documenting C2 compliance for the Unisys 4800 environment.

If you have any questions, please call Paul Cosgrave, Chief Information Officer at (202) 622-6800, or have a member of your staff call Dave Junkins, Director, Office of Information Resources Management, at (202) 283-4060 or Barry Herrmann, Chief, Office of IS Program Oversight, at (202) 283-7698, as appropriate.

Attachment

cc: Assistant Inspector General for Audit
Director, Audit Projects

**Attachment**

## Response to Draft Report the General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved

**Recommendation #1**

The Chief Information Officer should ensure that the 10 files we identified with taxpayer information are immediately secured to prevent systems users from casually reviewing the taxpayer data contained in the files without such access being reported to management.

**Assessment of Cause**

"Access to the 10 files was not reported to management since the files were incorrectly catalogued at a clearance level of zero instead of the proper clearance level 31." The only reason that those particular files were not reported to management is that they were at the wrong clearance level according to the auditor's selection of several additional files that were catalogued at a clearance level of zero and were assigned the production user-id (PROD) ACR in order to determine the readability of these files. Files with taxpayer information should always be at level 31, not zero. Management does not review zero level because they are systems files and/or software files and should not contain taxpayer data.

**Corrective Action #1**

The Assistant Commissioner, National Operations, and the Systems Support Division, in coordination with Security Standard and Evaluation, will review the 10 files and their interrelationship with other production files, to determine if it is feasible to secure the files without a major disruption of production activity in Andover and Austin Service Centers. Based upon this review, if it is determined that the files can be secured without a major disruption of production activity, appropriate actions will be determined and an action plan, with implementation dates, will be developed.

**Implementation Date for Corrective Action #1**

Completed: _____

Proposed: 01-01-2000

The Assistant Commissioner, National Operations, and the Systems Support Division, in coordination with Security Standard and Evaluation, will review the 10 files and their interrelationship with other production files, to determine if it is feasible to secure the files without a major disruption of production activity in Andover and Austin Service

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

Centers. Based upon this review, if it is determined that the files can be secured without a major disruption of production activity, appropriate actions will be determined and an action plan, with implementation dates, will be developed.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Recommendation #2**

The Chief Information Officer should ensure all systems files catalogued at clearance levels other than 31 that are readable by the casual system user are reviewed for the existence of taxpayer data. If identified, the files should be protected to ensure that casual accesses to files are either prevented or reported to management.

**Assessment of Cause**

In the Unisys 4800 environment it will be possible to limit access to files through improved use of Access Control Records (ACRs) in addition to the use of clearance levels. However, on the Unisys 2200 production environment any user who has been approved to access the production system are given clearance level 31, with the exception of Computer Operators and System Acceptability Test (SAT) programmers. All 31 level files are production files and therefore contain taxpayer data. These files must be accessed by management approved users and these accesses are reported to management on a routine basis. The term "casual" user is difficult to respond to since it is not related to a particular group of users as defined in the Unisys 2200 Standards.

**Corrective Action #2**

It is the responsibility of the file owner to determine the sensitivity of the data. Based upon the outcome of the analysis performed in corrective action #1, Security Standards and Evaluation will work with the Assistant Commissioner, National Operations, and the Systems Support Division to determine ownership. For any file below level 31, Security Standards and Evaluation will request that the owner provide the sensitivity of the file.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved**

**Implementation Date for Corrective Action #2**

Completed: _____

Proposed: 01/01/00
It is the responsibility of the file owner to determine the sensitivity of the data. Based upon the outcome of the analysis performed in corrective action #1, Security Standards and Evaluation will work with the Assistant Commissioner, National Operations, and the Systems Support Division to determine ownership. For any file below level 31, Security Standards and Evaluation will request that the owner provide the sensitivity of the file.

**Responsible Official**

Chief Information Officer IS
Office of Systems Standards and Evaluation IS:E

**Recommendation #3**

The Chief Information Officer should standardize control settings for files common to the Unisys 2200 production mainframes. Such a process should begin with the identification of files common to the Unisys 2200 production systems and a determination of the standard security attributes for each.

**Assessment of Cause**

"Analysis of these common files identified inconsistencies in access control settings for 11 to 13 percent of the files reviewed, depending on the control setting."

**Corrective Action #3**

The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation to identify the files common to the Unisys 2200 systems. Security Standards and Evaluation will coordinate this issue with other IRS organizations as the IRS migrates to a consolidated environment. Based on this review, the Assistant Commissioner, National Operations will be responsible for establishing and implementing standardized control settings for files common to the Unisys 2200 production mainframes.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Implementation Date for Corrective Action #3**

Completed: _____

Proposed: 06-01-2000
The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation to identify the files common to the Unisys 2200 systems. Security Standards and Evaluation will coordinate this issue with other IRS organizations as the IRS migrated to a consolidated environment. Based on this review, the Assistant Commissioner, National Operations will be responsible for establishing and implementing standardized control settings for files common to the Unisys 2200 production mainframes.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Recommendation #4**

The Chief Information Officer should ensure all improperly owned files are identified and assigned an owner present on the Unisys 2200 system at each service center, with the exception of files required to be unowned, prior to movement of that service center's mainframe to the consolidated Unisys 4800 environment.

**Assessment of Cause**

"All five systems reviewed contained both unowned files and files owned by user-ids that had been previously removed from the system."

**Corrective Action #4**

The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation to try to identify these files and develop a process to have these files profile modified prior to consolidating that particular center. SSE will review each site's files for improperly owned files as the consolidation process continues as well as in their normal process in performing their regular scheduled security reviews at these centers.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Implementation Date for Corrective Action #4**

Completed: _____

Proposed: 01-01-2001
The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation to try to identify these files and develop a process to have these files profile modified prior to consolidating that particular center. SSE will review each site's files for improperly owned files as the consolidation process continues as well as in their normal process in performing their regular scheduled security reviews at these centers.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Recommendation #5**

The Chief Information Officer should institute a policy requiring that all files owned by users being removed from the Unisys 2200 and Unisys 4800 systems either be deleted or assigned to a user present on the system.

**Assessment of Cause**

"IRM guidelines do not contain requirements for reassignment of file ownership after a user's removal from the system."

**Corrective Action #5a**

The Security Standards and Evaluation will work with the Assistant Commissioner, National Operations, and Systems Support Division to develop interim guidelines to address file ownership in the Unisys environment.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Implementation Date for Corrective Action #5a**

Completed: _____

Proposed: 06-01-2000
The Security Standards and Evaluation will work with the Assistant Commissioner, National Operations, and Systems Support Division to develop interim guidelines to address file ownership in the Unisys environment.

**Responsible Official**

Chief Information Officer IS
Office of Systems Standards and Evaluation IS:E

**Corrective Action #5b**

Within 90 days of receipt of the guidelines issued by Security Standards and Evaluation, the Assistant Commissioner, National Operations, will develop a requirements documentation - Request for Information Service (RIS) - requesting technical support from Systems Support Division to assist in the implementation of the guidelines.

**Implementation Date for Corrective Action #5b**

Completed: _____

Proposed: 10/01/00
Within 90 days of receipt of the guidelines issued by Security Standards and Evaluation, the Assistant Commissioner, National Operations, will develop a requirements documentation - Request for Information Service (RIS) - requesting technical support from Systems Support Division to assist in the implementation of the guidelines.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Corrective Action # 5c**

Within 180 days of receipt of recommendations from the Systems Support Division, the Assistant Commissioner, National Operations, will incorporate the necessary IRM guidelines for reassignment of file ownership to a present user after a user account is removed from the Unisys 2200 and 4800 systems.

**Implementation Date for Corrective Action # 5c**

Completed: _____

Proposed: 04/01/01
Within 180 days of receipt of the technical solution from the Systems Support Division, the Assistant Commissioner, National Operations, will incorporate the necessary IRM guidelines for reassignment of file ownership to a present user after a user account is removed from the Unisys 2200 and 4800 systems.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Corrective Action # 5d**

The Assistant Commissioner Service Center Operations will be responsible for implementing the guidelines for reassignment of file ownership in the Unisys environment for the service centers that have not been consolidated at the time of the completion of the actual guidelines. The Philadelphia Service Center is the final center scheduled for consolidation the first week of January 2001.

**Implementation Date for Corrective Action # 5d**

Completed: _____

Proposed: 06/01/01
The Assistant Commissioner Service Center Operations will be responsible for implementing the guidelines for reassignment of file ownership in the Unisys environment for the service centers that have not been consolidated at the time of the completion of the actual guidelines. The Philadelphia Service

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved**

Center is the final center scheduled for consolidation the first week of January 2001.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C Service Center Operations

**Corrective Action # 5e**

Martinsburg Computing Center (MCC) will implement IRM guidelines for reassignment of file ownership in the Unisys environment.

**Implementation Date for Corrective Action # 5e**

Completed: _____

Proposed: 02/01/02
Martinsburg Computing Center (MCC) will implement IRM guidelines for reassignment of file ownership in the Unisys environment.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O
Martinsburg Computing Center (MCC)

**Corrective Action # 5f**

Tennessee Computing Center (TCC) will implement IRM guidelines for reassignment of file ownership in the Unisys environment.

**Implementation Date for Corrective Action # 5f**

Completed: _____

Proposed: 02/01/02
Tennessee Computing Center (TCC) will implement IRM guidelines for reassignment of file ownership in the Unisys environment

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved**

**Responsible Organization**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O
Tennessee Computing Center (TCC)

**Recommendation #6**

The Chief Information Officer should examine the possibility of tracking individual user actions while using the MASTER user-id on the Unisys 4800 system and, if possible, implement this feature as soon as feasible.

**Assessment of Cause**

"The Unisys 2200 system does not possess a mechanism to monitor each user accessing the MASTER user-id."

**Corrective Action #6**

The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation in reviewing the possibility of relating the MASTER user-id to an individual human user within the security report. Also, as the sites are consolidated, the Security Standards and Evaluation will work with Systems Support Division to better define procedures on how to use the sub-system administrator option within the Unisys 4800 environment.

**Implementation Date for Corrective Action #6**

Completed: _____

Proposed: 06-01-2000
The Assistant Commissioner, National Operations, and the Systems Support Division are working with Security Standards and Evaluation in reviewing the possibility of relating the MASTER user-id to an individual human user within the security report. Also, as the sites are consolidated, the Security Standards and Evaluation will work with Systems Support Division to better define procedures on how to use the sub-system administrator option within the Unisys 4800 environment.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Recommendation #7**

The Office of Systems Standards and Evaluation management should issue a memorandum to all Unisys security analysts formally outlining the revised Unisys Access Standards deviation process.

**Assessment of Cause**

Review of the forms used to request modifications to standard Unisys 2200 system user profiles revealed that not all required signatures were present.

**Corrective Action #7**

In our 1998 security reviews, Security Standards and Evaluation identified that the centers were not in compliance with the Unisys 2200 standard. Also, in the summer of 1998 Security Standards and Evaluation contacted the Unisys Security Officer to remind them of the deviation process that must be followed. In addition, SSE formally issued a memorandum to the service centers and computing centers dated October 7, 1998, requiring any deviation to be documented and submitted to the National Office for review and approval.

**Implementation Date for Corrective Action #7**

Completed: 10/07/98 Proposed: _____
Security Standards and Evaluation formally issued
a memorandum to the service centers
and computing centers dated October 7, 1998, requiring
any deviation to be documented and submitted to the
National Office for review and approval.

**Responsible Official**

Chief Information Officer IS
Office of Systems Standards and Evaluation IS:E

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Recommendation #8**

The Chief Information Officer should ensure that all unapproved deviation forms are submitted to all required National Office functions for review and approval.

**Assessment of Cause**

"Discussions with National Office personnel also revealed that deviation forms had not been received by some of the specified functions. Also, during our security reviews last year, we identified lack of compliance with the 2200 Unisys Standards."

**Corrective Action #8**

Security Standards and Evaluation is working with the Assistant Commissioner, National Operations, to ensure that any deviations from the current 2200 Unisys Standards has documented and submitted to National Office for review and approval/disapproval.

**Implementation Date for Corrective Action #8**

Completed: 05/25/99 Proposed: _____

Security Standards and Evaluation is working with the Assistant Commissioner, National Operations Division (IS:O:O) to enforce that any deviation from the current 2200 Unisys Standards are documented and submitted to National Office for review and approval/disapproval.

**Responsible Official**

Chief Information Officer IS
Office of Systems Standards and Evaluation IS:E

**Recommendation #9**

The Chief Information Officer should ensure that all required C2 documentation is prepared for the Unisys 4800.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Assessment of Cause**

The IRS' Unisys 2200 systems are operating in a non-C2 compliant environment and without an approved waiver of compliance.

**Corrective Action #9**

The Service Center Mainframe Consolidation (SCMC) Project Office (PMO) has a task order with Science Applications International Corporation (SAIC) to develop this type of document. During Security Standards and Evaluation's security reviews, the lack of C2 documentation has been identified as a weakness. SSE staff is currently working with the PMO and the contractors to make sure this process is developed and tested for the new consolidated environment.

**Implementation Date for Corrective Action #9**

Completed: _____

Proposed: 06-01-2000
The SCMC Project Office (PMO) has a task order with Science Applications International Corporation (SAIC) to develop this type of document. During Security Standards and Evaluation's security reviews, the lack of C2 documentation has been identified as a weakness. SSE staff is currently working with the PMO and the contractors to make sure this process is developed and tested for the new consolidated environment.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations)
A/C National Operations IS:O

**Recommendation #10**

The Chief Information Officer should develop and maintain a security policy for the Unisys 4800.

**Assessment of Cause**

There is no security policy for the Unisys 2200.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

**Corrective Action #10**

Systems Standards and Evaluation will develop and maintain an IRS security policy for the Unisys 4800 in conjunction with the Service Center Mainframe Consolidation (SCMC) Project Office's (PMO) task order with Science Applications International Corporation (SAIC).

**Implementation Date for Corrective Action #10**

Completed: _____

Proposed: 01-01-2001
Systems Standards and Evaluation will develop and maintain an IRS security policy for the Unisys 4800 in conjunction with the Service Center Mainframe Consolidation (SCMC) Project Office's (PMO) task order with Science Applications International Corporation (SAIC).

**Responsible Official**

Chief Information Officer IS
Office of Systems Standards and Evaluation IS:E

**Recommendation #11**

The Chief Information Officer should conduct and document an assessment of the risk factors for the Unisys 4800.

**Assessment of Cause**

"While on-site, we asked whether a risk assessment had been performed on the Unisys 2200 environment. We were informed that no such assessment had been conducted specifically for the Unisys 2200. In addition, we were informed that no documentation exists of an IRS-wide assessment of any risk management factors for the Unisys 2200 environment."

**Corrective Action #11**

This process is part of the task order that the Science Applications International Corporation (SAIC) is working along with support from the Service Center Mainframe Consolidation (SCMC) Project Office's (PMO), Security Standards and Evaluation and other interested IRS organizations to conduct and document an assessment of the risk factors for the Unisys 4800.

**Response to Draft Report**
**the General Controls Environment over the Internal Revenue Service's**
**Unisys 2200 Systems Can Be Improved**

Completed: _____

Proposed: 06-01-2000
This process is part of the Task Order that the SAIC is working along with support from the PMO, SSE and other interested IRS organizations to conduct and document an assessment of the risk factors for the Unisys 4800.

**Responsible Official**

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS:O
Assistant Commissioner for National Operations IS:O:O