The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened

May 2000

Reference Number: 2000-20-072

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 9, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

OM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened

This report presents the results of our review of the general controls over the Internal Revenue Services' (IRS) Unisys 4800 system environment. In summary, we found that while access to these critical tax processing computer systems is adequately controlled, controls over user access within the system can be strengthened.

We recommended that the Chief Information Officer (CIO) should update current user access standards and develop new file access standards for the Unisys 4800 systems. In addition, the CIO should establish policies and procedures to improve security over console support systems and administration of system user profiles.

We issued a draft of this report to IRS management on March 20, 2000, with an April 20, 2000, response period. However, management's response was not available as of the date this report was released.

Please contact me at (202) 622-6510 if you have questions, or your staff may call Scott E. 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 4800 mainframe computer systems are a critical part of its tax processing system. These systems host databases used by the Integrated Data Retrieval System (IDRS), which enables IRS employees to have instantaneous visual access to many of the IRS' most sensitive taxpayer accounts. At the time of our review, these systems maintained an average of 7.7 million of these sensitive taxpayer accounts. In addition, these systems process tax returns for 3 of the IRS' 10 service centers before they are posted to the full taxpayer account on the IRS' Masterfile database. At the time of our review, the Unisys 4800 systems together processed an average of 13.2 million transactions per week, with an average of 58 transactions per second during peak hours of weekday processing.

Currently, the IRS is in the process of consolidating the mainframe operations of its 10 service centers into 2 computing centers. Once complete, the Unisys mainframes in production at each computing center will process almost all tax returns, which are expected to total 213 million in Fiscal Year 2000, and maintain all IDRS databases, which at the time of our review averaged 26.8 million taxpayer accounts.

The overall objective of this review was to evaluate the general controls over the IRS' Unisys 4800 computer system environment. Our review did not evaluate the controls over specific applications residing on the systems, since the IRS maintains a separate system to control most accesses to taxpayer accounts by its employees. The Unisys 4800 computer system environment[1] includes the production mainframes at the Martinsburg and Tennessee Computing Centers, as well as the disaster recovery mainframe at the Martinsburg Computing Center. The review was conducted in the Office of the Chief Information Officer, with on-site testing performed at both computing centers.

Results

Overall, the controls over access *to* the IRS' Unisys 4800 systems are adequate. Security policies are in place to authorize access to the system, with each user uniquely identified and authenticated by the system. Access to most sensitive taxpayer data files is monitored by management, and physical access to the system is restricted to authorized individuals. In addition, the IRS' consolidation of service centers has facilitated improvements in system controls and has resulted in greater accountability of user actions.

[1]The term environment is defined as both the mainframe's operating system and surrounding network.

Several areas were identified, however, where access controls *within* the systems were not adequate and where security can be improved. Access controls need to be strengthened over user access to and use of system programs and facilities, files, and other system resources. Such improvements are needed to ensure the confidentiality of taxpayer information stored on the systems, the availability of services provided by the systems, and the overall integrity of the systems.

A Majority of System User Profiles Are Not Compliant With Internal Revenue Service Guidelines

Approximately 80 percent of the system user profiles on both of the IRS' Unisys 4800 production systems are at least partially non-compliant with IRS guidelines for user access. As a result, these users are granted greater system access than that specified for their job responsibilities. Consequently, many of these system users are granted the ability to read, modify, delete, or manipulate system files or highly sensitive data. In addition, some system users are able to bypass many of the controls on the system and modify access controls for various system files. Contributing to the non-compliance of user profiles on these systems were the use of outdated guidelines for user access, the installation process for new users, and the granting of greater system access to users supporting the IRS' Mainframe Consolidation effort. Government and industry guidelines both specify that users for any system should be restricted to needed system resources.

Access to Critical System Files Is Not Adequately Controlled

Access to critical system files on the IRS' Unisys 4800 production and disaster recovery systems is not adequately controlled. Inadequate control over these files could result in users gaining access that would enable them to read, modify, or destroy application programs, system or data files, and transaction data. Although the IRS has issued guidelines for its Unisys system users, these guidelines do not specify access controls for files residing on these systems. Both Unisys system documentation and federal government guidelines specify that key system files should be restricted from unauthorized access.

Disabling Extended Security Controls Is a Security Risk

The access controls for the IRS' Unisys 4800 production systems are disabled on occasion during normal working hours to preserve security records for users who are removed temporarily from the system. Disabling these Extended Security controls could provide system users with unauthorized access to sensitive files and allow them to harm the system, either intentionally or inadvertently, by modifying or deleting critical system files.

Control Weaknesses With the Single Point Operations System Place the Unisys 4800 Systems at Risk

The IRS' Unisys 4800 mainframe environment is supported by a Unix-based Single Point Operations (SPO) system that enables mainframe operations to be centrally monitored and controlled at each computing center. We identified several control weaknesses that could compromise the security of the SPO system and potentially allow unauthorized individuals to alter or halt operation of the Unisys 4800 system. We determined that this system does not have an overall security policy, which is required by IRS procedures for systems containing sensitive information.

User Access Control Can Be Improved by Increasing the Minimum User Password Length

The minimum length of user passwords for the IRS' Unisys 4800 systems is set too low to adequately safeguard the systems. While meeting password length requirements specified by federal standards for information processing, the systems do not meet more recent General Accounting Office (GAO) guidelines for password length.

Summary of Recommendations

Based on these results, we recommend several actions that can strengthen control over the IRS' Unisys 4800 systems. The Chief Information Officer should revise the Unisys Access Standards and implement them in a standardized manner while providing a schedule for their periodic review and update. In addition, standards should be developed that define access to sensitive files on the systems, policies should be established to reduce the risk of disabling system access controls, and security procedures should be developed for the SPO system. To increase user security over the system, the minimum password length on the Unisys 4800 systems should be increased to meet GAO guidelines.

We issued a draft of this report to IRS management on March 20, 2000, with an April 20, 2000, response period. However, management's response was not available as of the date this report was released.

Objective and Scope

This report presents the results of our review of the Internal Revenue Service's (IRS) Unisys 4800 mainframe system environment. The objective of this review was to evaluate the general controls over this environment;[1] however, the controls over specific applications residing on these systems were not evaluated as part of this report. Many of these applications are controlled by a separate system, the IRS' Security and Communications System.

We evaluated system policies as well as physical and logical access controls of the Unisys 4800 system environment. The systems evaluated in this review were the two production mainframe systems at the Martinsburg (MCC) and Tennessee (TCC) Computing Centers, as well as the disaster recovery mainframe system at the MCC.

Audit work was conducted in the Office of the Chief Information Officer from April to November 1999. Audit tests and observations were also conducted on-site at the MCC and the TCC. This audit was performed in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II. Additional technical details of issues discussed in this report are listed in Appendix IV. Appendix V contains a glossary of terms used in this report.

Background

The IRS' Unisys 4800 mainframe systems are a critical part of its tax processing system. These systems host databases used by the Integrated Data Retrieval System (IDRS), which enables IRS employees to have

[1] The term environment is defined as both the mainframe's operating system and surrounding network.

instantaneous visual access to many of the IRS' most sensitive taxpayer accounts. The IDRS database on the Unisys 4800 systems maintained an average of 7.7 million accounts and 13.4 million related account records during July 1999.

The Unisys 4800 mainframe systems currently process tax returns for three service centers before they are posted to the full taxpayer account on the IRS' Masterfile database.

In addition, the Unisys 4800 systems currently process tax returns filed by taxpayers at three service centers before the returns are posted to the full taxpayer account on the IRS' Masterfile database. At the time of our review, these systems processed an average of 2.5 million transactions per day, with an additional 715,000 transactions processed per weekend. During peak hours of weekday processing, the IRS' two Unisys 4800 production systems together processed an average of 58 transactions per second. Peak hours of weekday processing workload were determined to be from 10AM to 12PM and 1PM to 3PM.

Currently, the IRS is in the process of consolidating the mainframe operations of its 10 service centers into 2 computing centers. Once consolidation is complete (projected to be January 2001) each of the two Unisys 4800 production systems will process transactions from and host IDRS databases for five service centers. At the time of our review, all IDRS databases in the service centers and the computing centers contained a total of 26.8 million of the most sensitive taxpayer accounts and 44.4 million related taxpayer account records. For Fiscal Year 2000, the IRS expects to receive 213 million tax returns.

Results

While access controls to *the Unisys 4800 systems are adequate, access controls* within *the systems can be improved.*

Our review of the general controls over the Unisys 4800 systems determined that while access controls *to* the system are adequate, access controls *within* the systems could be improved. Access controls to the systems are used to verify that users attempting to access the systems are authorized. Access controls within the systems specify the mainframes' resources available to authorized system users.

Our review of access controls *to* the systems determined that:

- Security policies are in place to authorize access to the system, and each user is uniquely identified and authenticated by the operating system.
- Access to most sensitive taxpayer data files is monitored by management.
- Physical access to system hardware, as well as primary system consoles, is restricted to authorized individuals.
- Controls over the security officer user profiles are adequate.
- Devices used to encrypt data transmitted into and out of the MCC and the TCC are active and operating in a secure mode.
- Procedures for backing up system data and files are adequate.

In addition, we identified areas where the IRS' consolidation of service center mainframe operations has facilitated improvements in system controls. For example, management reports of user accesses have been restructured to provide greater accountability by assuring user accesses are reported to the front-line managers. In addition, all actions by non-operational users, such as contractors and system support personnel, are being specifically monitored.

In general, access controls can be strengthened over user access to and use of system programs and facilities, files, and other system resources.

Our review of access controls *within* the systems, however, identified several areas where controls were not adequate and where security can be improved. Generally, access controls can be strengthened over user access to and use of system programs and facilities, files, and other system resources. Such improvements are needed to ensure the confidentiality of taxpayer information stored on the systems, the availability of services provided by the systems, and the overall integrity of the systems.

A previous Treasury Inspector General for Tax Administration report[2] identified a control weakness on several of the IRS' Unisys 2200 mainframe systems that enabled system users to read taxpayer data without these accesses being reported to their managers. We identified a similar situation on the Unisys 4800 system at the MCC. This weakness was reported on-line to the appropriate security personnel at the MCC. In response, the security administrators for the system modified one of the system user profiles, which significantly improved control over these files.

A Majority of System User Profiles Are Not Compliant With Internal Revenue Service Guidelines

Approximately 80 percent of the system users on both of the IRS' Unisys 4800 production systems are granted greater system access than that specified for their designated job responsibilities.

Approximately 80 percent of the system users on both of the IRS' Unisys 4800 production systems are granted greater system access than that specified in the IRS guidelines for their designated job responsibilities. As a result, many of these system users are granted the ability to read, modify, delete, or manipulate system files or highly sensitive data to which they do not need access. In addition, some system users are able to bypass many of the controls on the system and modify access controls for various system files.

Each system user on the Unisys 4800 is associated with a profile, which specifies the system accesses granted to the user and is defined by the user's job responsibilities. Profiles consist of a series of settings that grant access to specific system resources and commands. The IRS has developed guidelines, in the form of Access Standards, which specify many of these settings for groups of users with similar job responsibilities.

[2] *The General Controls Environment Over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved (*Reference Number 199920063, dated August 1999)

Through comparison of the settings in each user's profile with those specified in the Access Standards (for the user's job responsibility), we determined that approximately 45 percent of the settings were not compliant with the IRS' Access Standards.[3] Approximately 80 percent of all system users on both of the IRS' Unisys 4800 production systems have at least one non-compliant setting.[4] Although there were a significant number of user profiles in non-compliance with the Access Standards, many of the profiles contained relatively few non-compliant settings.

Table 1 summarizes our results by production system at each computing center:

Results	MCC	TCC
Total number of system users	426	361
Percentage of system user profiles in non-compliance with the IRS' Unisys Access Standards	77.2%	85.6%
Percentage in non-compliance with the Access Standards for five or fewer profile settings	42.7%	52.4%
Total number of settings in all user profiles	12,728	7,269
Percentage of profile settings in non-compliance with the Access Standards	46.1%	42.3%

Table 1: Summary of non-compliance results by production system

Although several factors contributed to the non-compliance of user profiles on the IRS' Unisys 4800 systems, one primary factor is the limited usefulness of the IRS' Unisys Access Standards. These Standards have been in effect since March 1996 and were last updated in July 1996. Security administrators use these Standards as guidelines in defining profiles for

[3] As of September 10, 1999.

[4] Sixty-two user-ids from both production systems did not fit into any of the Unisys Access Standards profile categories and, therefore, were not included in the assessment.

new system users. However, the IRS' migration from the Unisys 2200 platform to the Unisys 4800 platform has resulted in the need to grant additional system accesses to some users in order for them to effectively perform their job responsibilities. As a result, security administrators currently do not have a viable standard to reference for many users and, consequently, have difficulty defining the proper profile for them. Neither the Standards nor IRS procedures require the Standards to be reviewed or updated on a periodic basis to ensure their appropriateness.

Contributing to the non-compliance of user profiles on these systems were the use of outdated guidelines for user access, the installation process for new users, and the granting of greater system access to users supporting the IRS' Mainframe Consolidation effort.

Additionally, the following factors also contributed to the non-compliance of user profiles on the IRS' Unisys 4800 systems, many of which stem from the IRS' Unisys Mainframe Consolidation effort:

- **User Installation Process:** The security software on the Unisys 4800 systems permits new user profiles to be created by copying an existing user profile on the system. Security personnel for these systems informed us that this was a common practice for installation of new users. Although more efficient, this process propagates any non-compliant settings from the existing user profile to those being added to the system.
- **Mainframe Consolidation Transition:** In support of the IRS' Unisys Mainframe Consolidation effort, certain types of users are authorized to be granted profiles with greater system access than normal. For example, both contractors and system software personnel have been profiled as Database Administrators (DBA), who have nearly unrestricted access to the system, for the duration of the IRS' Mainframe Consolidation effort. Standard profiles for these users in the IRS' Access Standards are more restrictive, prohibiting, for example, all privileges that bypass system access controls.
- **System-Forced Profile Setting Not Specified in the Standards:** Included in many of the user profiles on both production systems are two settings that the system forces to be granted in combination. The IRS' Unisys Access Standards specifies one of

these settings for several user profiles; however, few profiles are specified with the other setting. Consequently, most of the users with the latter setting were determined to be non-compliant with the Access Standards.

The IRS' Unisys Access Standards specify a process for requesting and approving exceptions from the Standards for individual users. Our review of the exception requests found that, out of a random sample of 64 user profiles from the 638 user profiles we identified to be non-compliant with the Standards, only 5 user profiles had approved exception requests. Although most of the exceptions in our sample were not approved, we observed approved requests for users with similar job responsibilities. These users, in general, were supporting the IRS' Unisys Mainframe Consolidation effort. The approval for these exception requests generally expires when the Consolidation effort is completed.

Both government and industry guidelines suggest that, to remain effective, access policies should be in place and maintained.

Both government and industry guidelines suggest that, to remain effective, access policies should be in place and maintained. Specifically:

- The General Accounting Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) specifies that an entity "should identify the specific user or class of users that are authorized to obtain direct access to each [system] resource for which [each user] is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties." The FISCAM document also specifies that these access authorization listings should be reviewed periodically to determine whether they remain appropriate.
- The Governance, Control, and Audit for Information and Related Technology (CobiT)[5] document, issued by the Information Systems Audit and Control Association, suggests that access to and use of

[5] CobiT is a generally accepted standard for information technology security and control practices.

computing resources should be restricted by the implementation of an adequate authentication mechanism of identified users and resources associated with access rules. Procedures should also be in place to keep authentication and access mechanisms effective.

Recommendations

1. The Chief Information Officer (CIO) should revise the Unisys Access Standards to reflect the changes resulting from both the IRS' Mainframe Consolidation effort and the migration to the current version of the Unisys 4800 operating system.
2. The CIO should implement the revised Unisys Access Standards in a standardized manner, such as through user profile templates that can be copied to install new users. Such templates should mirror the Access Standards and be disabled or otherwise prevented from being accessed by unauthorized personnel.
3. The CIO should modify non-compliant user profiles to make them compliant with the revised Unisys Access Standards. Any remaining non-compliant user profiles should have an approved deviation request.
4. The CIO should establish a schedule for reviewing and updating the Unisys Access Standards to ensure their appropriateness.

Management's response was not available at the time this report was released.

Access to Critical System Files Is Not Adequately Controlled

Access to critical system files on the IRS' Unisys 4800 production and disaster recovery systems is not adequately controlled. Inadequate control over these

files could result in users gaining access that would enable them to read, modify, or destroy application programs, system or data files, and transaction data.

Unisys mainframe systems have the capability of defining access controls for both system users and system files; however, the IRS' Access Standards provide guidance only for profiling system users.

Unisys mainframe systems have the capability of defining access controls for both system users and system files. As mentioned previously, system users are granted access within the system based on their user profile. Access controls over system files are also defined through a profile, which specifies the user profile settings needed to access the file. Consequently, if the profiles for both a user and file do not match, access to the file is restricted. As discussed previously, the IRS' Unisys Access Standards specify profiles for several types of users; however, the Standards do not specify profiles for any system files.

Our review identified two types of critical system files for which access controls were inadequate: system libraries and operating system files. Each type of file is discussed in the following sections.

System Libraries

System libraries are critical to the operation of the IRS' Unisys systems; however, nearly 93 percent of the libraries permitted any system user to access the library and use the software product contained in it.

System libraries are critical to the operation of the IRS' Unisys systems, as they contain all components of the software products installed on the system. Access to some system applications and utilities is also controlled through access to these libraries. Of the 858 system libraries on the IRS' Unisys 4800 production and disaster recovery systems, nearly 93 percent were secured in such a way that any system user could access the library and use the software product contained in it.

Table 2 summarizes the system libraries accessible by all system users:

System	Number of system libraries	Percentage of system libraries accessible by all users
TCC production	263	89.2%
MCC production	267	95.4%
MCC disaster recovery	266	94.0%

Table 2: Summary of system libraries accessible by system users

Many system libraries contain sensitive programs to which access should be restricted.

Many of these libraries contain sensitive programs to which access should be restricted, such as compilers, job schedulers, file administration programs, and software installation and maintenance programs. While many users need access to specific libraries as part of their job responsibilities, most do not. For example:

- Access to operating system software is typically permitted only to system programmers who modify the system or intervene when it is not working properly.
- Access to database management software is permitted only to DBAs.
- Access to security software is permitted only to senior-level security administrators.
- Access to system software is not permitted to application programmers and computer operators, since it is incompatible with their duties.

Default access controls are set on the IRS' Unisys 4800 systems to grant all users the ability to read and run all programs in the system libraries.

Access control to system libraries is established when the library is first installed on the system. The software products used to install the system libraries define the default access controls for the library. We were informed by system security personnel that the default access controls for system libraries are set to grant all system users the ability to read and run all programs in that library.

After installation of the system library, default access controls can be modified by the system administrator.

Such modifications by the systems administrator include adding access lists to the system libraries, which specify the users permitted to read, write, modify, or delete the library. For many systems libraries, however, access lists have not been developed to further restrict access to specific users.

Operating System Files

Access control over two important system files on the MCC production system is inadequate, which gives many system users the ability to modify or delete the files.

Access control over two important system files on the MCC production system is inadequate, which gives many system users the ability to modify or delete the files. These files are 2 of the 14 control and security files that are critical to the operation of the system. The same files are properly secured on the Unisys 4800 disaster recovery system at the MCC and the production system at the TCC with an access list permitting read-only access.

This issue was raised to both National Office and MCC security personnel, who subsequently added the appropriate access list to the files. As a result of this on-line correction, no further corrective action for these specific system files is required.

Unisys operating system documentation specifies how both types of files should be secured. Specifically:

- All system libraries should be protected from unauthorized access, such as through an access control list.
- All system files are cataloged with a specified access list permitting read and execute access to the system files while preventing write and delete access.

The GAO's FISCAM document recommends that "access to system software should be restricted to a very limited number of personnel whose job responsibilities require that they have such access." The FISCAM document defines system software as operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Recommendation

5. The CIO should establish access standards on the Unisys 4800 for system software and other sensitive system and data files, specifying appropriate access controls for these files and the types of users that should be granted access to them.

Disabling Extended Security Controls Is a Security Risk

Disabling Extended Security controls creates the potential for a system user to access files or inadvertently harm the system.

The access controls for the IRS' Unisys 4800 production systems are disabled on occasion during normal working hours. Disabling these Extended Security controls creates the potential for a system user to access files, sensitive or otherwise, or inadvertently harm the system, such as by modifying or deleting critical system files. Normally, system users are unaware that Extended Security has been disabled. However, the system does permit users to identify if Extended Security has been disabled.

Security personnel for the Unisys 4800 systems informed us that Extended Security is disabled in situations where users are removed from the system, but will be added at some later time. This requires that the security record for the user's profile be preserved, which requires the user to be removed when Extended Security is disabled. Security personnel at the MCC informed us that this is the method they use when users no longer need access to the system. They also informed us that Extended Security is disabled on an average of once a week for a short period of time.

Users can be disabled instead of deleted. This action can be done while Extended Security controls are active.

The IRS' Unisys mainframe systems also permit users to be disabled instead of being removed from the system. This option does not require Extended Security to be disabled. TCC security personnel informed us that this is the method they use when users no longer need access to the system. Consequently, they have disabled Extended Security only on rare occasions.

Although there is a difference in the methods for restricting user access by security personnel at each computing center, each method has its merits. For example, some users require periodic access to the system. In this case, disabling user access would be an easier and more secure method, since Extended Security can remain active. It would also reduce the time needed by the security administrators to later add the user to the system. However, there are also users who need one-time access to the system. In this case, the user should be removed from the system. For this and other instances when Extended Security is disabled, it should be done for a minimal amount of time and at a time when few users are accessing the system.

IRS procedures require Information Systems functions to ensure that adequate security is provided for all data collected, processed, transmitted, stored, or disseminated on information systems and networks. The procedures also require security administrators to add and delete user access; however, no provision is specified for disabling user access.

Recommendations

6. The CIO should establish procedures specifying the appropriate method for deactivating user profiles on the Unisys 4800 systems.
7. The CIO should establish procedures specifying when disabling Extended Security on the Unisys 4800 systems is permitted. The procedures should also specify that Extended Security should be disabled at a time when user accesses to the system are minimal, such as during off-peak hours or weekends.

Control Weaknesses With the Single Point Operations System Place the Unisys 4800 Systems at Risk

The IRS' Unisys 4800 mainframe environment is supported by a Unix-based system that enables

mainframe operations to be centrally monitored and controlled. This Single Point Operations (SPO) system[6] is also used to automate operations of the Unisys mainframes at each computing center and eventually alert system operators of any problems in the environment.[7] The SPO system is able to accomplish this by linking all Unisys mainframe consoles at each computing center and providing a single integrated console for system management. Control weaknesses affecting the SPO system may, in turn, adversely affect the IRS' Unisys mainframe operations.

Several control weaknesses were identified on the SPO system that could potentially compromise its security.

We identified several control weaknesses that could potentially compromise the SPO's system security and allow unauthorized individuals to alter or halt operation of the Unisys 4800 system. While some weaknesses were identified on the SPO servers at both computing centers, others were found in the system environment at the TCC only. Specifically:

- **Insecure File Transfer Method:** The SPO servers at both computing centers use a file transfer method that permits most system files to be transferred without user identification or authentication. The SPO servers use this method to transfer operating system software to terminals on the computer floor. This method can be better secured by restricting such file transfers to specified system files.

Insecure file transfer methods and inadequate controls over access to the SPO application were identified on the SPO systems at both computing centers.

- **Inadequate access control to the SPO application:** All of the operators at each computing center use the same operator user logon and password to access the SPO application. Similarly, all administrators for the system use the same administrator user logon. As a result, actions of individual users cannot be identified from either the system log or the application log.

[6] The SPO system is comprised of servers, a SPO console, remote consoles, Unisys system consoles, and the adjoining network.
[7] The alert function of the system was not fully functioning at the time of our review; however, it was in the process of being configured.

- **Infrequent change of sensitive password:** At the time of our review, the system administrator's password, or *root* password, on the TCC SPO server had not been changed since September 1997. In addition, this password was the same for 10 other users on the system. As a result, there is a strong likelihood that this sensitive password would be known by multiple users, giving them the capability to access the entire system without their individual accesses being identified in the system log. After this issue was raised, the system administrator agreed to change the password.

- **Infrequent review of the superuser (su) log:** Unix-based systems record various user and system actions on several system logs. One such log, the *su* log, is used to identify unauthorized access. At the time of our review of the TCC SPO server, this log had not been reviewed for several weeks. Our review identified numerous unsuccessful accesses to the TCC server, which were later determined to be from another IRS system. Unless the *su* log is reviewed on a frequent basis, efforts to compromise the system will not be identified in a timely manner. In the case of the *root* or other sensitive account, such access could compromise system security and integrity.

- **Input devices on Unisys system consoles are not adequately secured:** The IRS' Unisys system consoles are workstations that are used to control operations of its Unisys mainframe systems, including initiating or ending jobs and starting or shutting down the system. At both computing centers, these computers are located in a computer room, access to which is controlled by management, and overseen by operators at all times. However, at the TCC, the consoles are connected to active modems, which can be used to remotely access the console. In addition, the consoles are not physically secured inside the computer room. Conversely, at the MCC, system consoles were locked from use in a cabinet, with the modems disconnected and stored in a separate location.

Securing input devices on system consoles reduces the likelihood that the integrity and security of the consoles would be compromised.

Securing these consoles reduces the likelihood that the integrity and security of the consoles would be compromised, such as through the introduction of computer viruses or modification of the console operating system. Such compromises could lead to the halting of the operation of the Unisys mainframe systems at the TCC.

- **TCC network configuration does not prevent access to the SPO server:** At the MCC, access to the SPO system is restricted not only through application controls but also through access lists placed on the network. These additional controls prevent users from establishing system consoles outside of the computer room, where users without the need to view or access the system console may be able to do so. On the other hand, the TCC network does not restrict access to the SPO system through the network, relying instead, on access controls in the SPO application. As stated previously, we found this control to be inadequate.

There is no overall security policy for the SPO system.

Through discussions with system administrators, we determined that there is no overall security policy for the SPO system. In addition, the MCC system administrator has responsibility for two functions which should be separated: system and security administration. Also, not all security administrators had received training necessary to adequately administer security for the SPO systems.

IRS procedures require the establishment of a computer security plan for all information systems that contain sensitive information.

IRS procedures require the establishment of a computer security plan for all information systems that contain sensitive information. IRS procedures also define sensitive information as that which requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction. In our view, this includes not only the systems that store and process sensitive information but also those that support such sensitive systems.

IRS procedures also require that individual duties and responsibilities in a critical function be separated. This

separation of duties will prevent a single individual from corrupting a critical process.

Recommendations

8. The CIO should assess the security of the SPO system and surrounding network at both computing centers and develop security procedures for the SPO systems.
9. The CIO should segregate the system and security administration functions over the SPO system.
10. The CIO should ensure that all security administrators are provided with adequate training in how to provide proper administration of the system.

User Access Control Can Be Improved by Increasing the Minimum User Password Length

The minimum length of user passwords for the IRS' Unisys 4800 systems is set too low to adequately safeguard the systems.

The minimum length of user passwords for the IRS' Unisys 4800 systems is set too low to adequately safeguard the systems. At the time of our review, passwords on these systems were required to be at least four characters in length. At this length, the combination of possible passwords using alphanumeric characters is 1.4 million. However, increasing the minimum password length to 6 characters increases the number of possible password combinations to 1.4 billion, significantly reducing the risk of someone guessing the password and obtaining unauthorized access to the system. The IRS appears to have kept the minimum password length in the Unisys 4800 system environment the same as that used in the prior Unisys 2200 system environment.

GAO guidelines recommend that passwords be at least six characters in length to reduce the chances of being easily guessed.

The Federal Information Processing Standards (FIPS) require that passwords be at least four characters in length for all systems. For medium protection systems, such as IRS systems, the FIPS specify that password lengths should range between four and eight characters. More recent guidance from the GAO's FISCAM document recommends that password lengths be at least

six characters to reduce the chances of being easily guessed.

Recommendation

11. The CIO should increase the minimum password length on the Unisys 4800 systems to at least six characters.

Conclusion

Strong controls are needed over the IRS' Unisys 4800 mainframe environment to both protect taxpayer information and ensure that such information is processed accurately and available when needed.

The IRS' Unisys 4800 mainframe systems are critical to its ability to process tax returns. Strong controls are needed over this environment not only to protect taxpayer information but also to ensure that such information is processed accurately and is available when needed. With the IRS expected to consolidate mainframe operations of the remaining service centers by 2001, these systems will become even more critical to the IRS' tax processing system. Therefore, it is imperative that these systems have a strong control environment.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the general controls over the Internal Revenue Service's (IRS) Unisys 4800 system environment. This environment is comprised of each production mainframe system at the Martinsburg (MCC) and Tennessee (TCC) Computing Centers, as well as the disaster recovery mainframe at the MCC. During this review, we evaluated system policies as they relate to security, identification and authentication controls, access controls, and physical security at each site.

Specifically, we:

I. Obtained background information on the Unisys 4800 system and its security requirements.

   A. Reviewed system manuals and other documentation to gain an understanding of the system.

   B. Reviewed applicable System Information Bulletins and other IRS documentation to identify requirements for Unisys 4800 systems.

   C. Reviewed previous Treasury Inspector General for Tax Administration and General Accounting Office reviews on the IRS' Consolidation efforts.

   D. Reviewed relevant Office of Management and Budget regulations and Department of the Treasury directives regarding systems security.

   E. Identified the number of users with direct access to the Unisys 4800 mainframes.

   F. Identified the volume of transactions being processed by the Unisys 4800 mainframes on a daily and hourly basis.

II. Assessed the adequacy of system security policies.

   A. Reviewed the adequacy of the security management structure over the systems.

   B. Reviewed the adequacy of security-related personnel and training policies.

III. Evaluated the adequacy of system access controls.

   A. Determined the operating system level implemented.

   B. Determined whether System Security is enabled and which Security Option is installed.

   C. Evaluated the adequacy of access and removal policies over system users.

D. Evaluated the appropriateness of user privileges and verified their compliance with the IRS' Unisys Access Standards.

E. Evaluated controls over the system console.

IV. Evaluated usage of and control over privileged user accounts.

A. Determined who has system administrator privileges and how this privilege is restricted.

B. Evaluated the controls over the security administration user profile.

V. Evaluated appropriateness of user password settings and policies. Determined whether:

A. Password options are being used appropriately for each production system.

B. Initial passwords expire when an administrator sets up a password for a user.

C. The security system restricts passwords from easily being guessed.

D. Passwords are stored in a protected file in a non-readable format and do not appear visibly on screens.

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

A. Identified the control structure in place over file access.

B. Determined whether there are any uncatalogued files on the system.

C. Assessed controls over sensitive system files.

D. Assessed user policies over file access controls.

E. Determined if Unisys has provided operating system source code to the IRS and assessed the controls in place to ensure that only authorized individuals have access to the code.

F. Determined what controls are in place over the Access Locator Number source code.

VII. Assessed controls over local network or dial-up connections.

A. Determined how data and programs are transported through telecommunications lines and assessed security, integrity, and configuration controls, including the Single Point Operations sub-network.

B. Determined whether devices used to encrypt data transmitted into and out of the MCC and the TCC were active and operating in a secure mode.

VIII. 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. Assessed system controls over the audit trail.
- C. Determined whether system audit logs are reviewed and the frequency of review.
- D. Attempted to access files to which users do not have access based on the permissions information obtained in the previous step.

IX. Determined whether database back-up and recovery procedures have been developed, implemented, and tested and assessed the adequacy of the procedures.

X. 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 its adequacy.
- C. Assessed the security surrounding the system console.
- D. Observed physical security over user and developer terminals.
- E. Assessed controls over the tape/media library.
- F. Evaluated emergency measures in place for the computer room.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Vincent J. Dell'Orto, Audit Manager
Michael Howard, Senior Auditor
Arthur Granger, Auditor
Andrew Harvey, Auditor
Gerard Marini, Auditor
Nikki Thomas, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Deputy Chief Information Officer (Operations) IS
Director, Enterprise Operations IS:EO
Director, Information Resources Management IS:IR
Director, System Support IS:SS
Director, Martinsburg Computing Center IS:EO:MC
Director, Tennessee Computing Center IS:EO:TC
Director, Office of Security and Privacy Oversight IS:SPO

Appendix IV

Additional Technical Information

This appendix includes technical information not specified in the body of the report but which may be useful to Internal Revenue Service (IRS) management.

A Majority of System User Profiles Are Not Compliant With Internal Revenue Service Guidelines

Methodology

The assessment of compliance of user profiles with the IRS' Unisys Access Standards included a comparison of most, but not all, of the controls specified in the Standards. The excluded controls were those that changed in the process of migrating to the Unisys 4800 environment, such as accounts and console message groups. The controls that were included in the assessment were:

- Access Allowed
- Minimum Clearance Level
- Maximum Clearance Level
- Console Mode
- Console Keyins
- Privilege Keywords
- Executive Request Keywords

The source of the user profile settings was the SIMAN User-ID Maintenance Keyword Reports. The assessment was essentially a comparison of these reports to the Unisys Access Standards, using the Access Standards categories as a common point of reference. Each user in the reports was categorized according to the user's job function and placed in the appropriate Access Standards category, as is generally done when new users are added to the system. Further discussions were held with security personnel at the Martinsburg Computing Center (MCC) and the Tennessee Computing Center (TCC) to determine whether user-ids were properly categorized. Deviations were identified for each user-id by comparing the user-id's actual profile on the system with that specified in the Access Standards, using the Access Standards category as a common point of reference. Due to ambiguity in the Access Standards, we were not able to categorize 62 users on both systems. These users, which were excluded from the assessment, appeared to have either file transfer, system, National Office, or Service Center profiles.

System-Forced Profile Setting

One of the causes identified for some of the user profile deviations was the assignment of two privileged interfaces that the system forces to be granted in combination, PB$CON and CONNECT$TIP. PB$CON is specified for many user profile categories in the Unisys Access Standards, whereas CONNECT$TIP is not.

Access to Critical System Files Is Not Adequately Controlled

System Library Files

As stated in the report, access to most of the system libraries on the IRS' Unisys 4800 production and disaster recovery systems is not adequately controlled. These system libraries are files with the qualifier SYSLIB. Through review of the clearance levels and access control records (ACR) for the files, we determined that these files were accessible by any system user. The libraries we identified that were readable were cataloged at clearance level 0, did not have an ACR assigned, and were designated as PUBLIC.

We determined that these libraries were secured in this manner because the software installation products (COMUS or SOLAR) used to install the libraries had set a default file security option that enabled at least read access by system users. These options specify the access control settings for a new software product when installed on the system. Our research of these options identified three possible settings:

- NONE: Each product is cataloged without an ACR and designates the system libraries as PUBLIC.
- KEYS: Each product file is cataloged as PUBLIC with a random write key.
- PRIVATE: Each product file is cataloged as PRIVATE.

Operating System Files

The two operating system files referenced in the report that were not properly secured on the MCC's Unisys 4800 production were SYS$*DLOC and SYS$*ILES$. These two files were cataloged on the MCC's Unisys 4800 disaster recovery system and the TCC's production system with the ACR ACRRO, which permits read-only access to system users.

Control Weaknesses With the Single Point Operations System Place the Unisys 4800 Systems at Risk

The insecure file transfer method referenced in the report is the trivial file transfer protocol (TFTP). This protocol is a less secure version of the FTP protocol because TFTP does not require a user to enter a user-id or password. Our research identified that this protocol can be better secured by restricting the file transfers to a specified directory. This is done by implementing a –s or –r option followed by the directory name in the network configuration file */etc/inetd.conf*. In the case of the Single Point Operations system, this would restrict all transfers to only the operating system software needed to boot terminals on the computer room floor.

Appendix V

Glossary of Terms

Term	Definition
Access Controls	A series of system mechanisms and processes that validate whether a user is authorized to access the system and, if so, the system resources the user is permitted to use.
Application	A series of computer programs that enable users to perform specified tasks. Examples include word processors, spreadsheets, and web browsers.
Application Controls	Specific program controls that ensure that transactions are valid, properly authorized, and completely and accurately processed.
CobiT	The Control Objective for Information Technology document, which provides guidance, rules, and regulations for information technology security programs. An accepted industry standard, CobiT is published by the Information Systems Audit and Control Association.
Compiler	A computer program that translates computer instructions into a form that a computer can understand and execute.
Computing Center	Internal Revenue Service (IRS) Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
Database Management Software	A series of programs that enable users to store, modify, and extract information from a database.
Disaster Recovery System	An emergency backup computer that is used for operations when an existing production system is disabled, such as through a natural disaster.
Extended Security	The term used to describe a set of critical access controls on the Unisys 4800 system.
File Administration Program	A series of programs that maintain files on a computer. These programs manage file backups and the location of files for the most efficient use of disk space, among other functions.
FISCAM	The Federal Information System Controls Audit Manual, which is a guidance document published by the General Accounting Office.

Integrated Data Retrieval System (IDRS)	An IRS computer system that is capable of retrieving or updating stored information from taxpayers' account records.
Job Scheduler	A series of programs that allow the computer to schedule jobs without the regular intervention of users.
Masterfile	The IRS' database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
Operating System	Software for all computers that is used to manage, control, and allocate its hardware resources.
Operating System Software	Software that enables a computer to perform basic tasks, such as reading input from devices (such as a keyboard), directing output (such as to a monitor or printer), and recognizing and managing all attached devices (such as disk drives and printers). It is the most important set of programs on a computer.
Production System	A system that processes and stores data actively used by an organization. In contrast, test and disaster recovery systems are used only to test programs for production systems or replace them in emergency situations, respectively.
Security Software	Software installed in the system with the purpose of controlling system access (authentication of users).
Service Center	The data processing arm of the IRS. The service centers process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
SIMAN	The Site Management Complex, which is the security software present on the Unisys 4800 mainframe system.
Software Installation and Maintenance Program	A series of programs used to install, configure, and remove software products on a computer.
SPO	The Single Point Operations system links all Unisys mainframe consoles at each computing center and provides systems management from a single integrated console.
System Console	A computer, typically a personal computer, that is used to monitor and control the operation of a mainframe.

System	For purposes of this report, system environment includes the operating

Environment	system and surrounding network of the Unisys 4800 mainframe systems.
System Libraries	Files that contain all components of the software products installed on a Unisys 4800 mainframe system.
System User	An individual who is authorized to access the operating system of a computer. In contrast, application users are granted access to only a specific application on a system.
Unisys Access Standards	Requirements issued by the IRS specifying the access controls granted to system users on the IRS' Unisys mainframe systems.
Unix-based system	A computer that uses the Unix operating system.
User Profile	A series of access control settings that define the system resources a user is permitted to use.