

**Controls Over the Masterfile System
Are Generally Adequate, But Some
Improvement Is Needed**

June 2001

Report Number: 2001-20-092

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

June 18, 2001

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION/
CHIEF INFORMATION OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Controls Over the Masterfile System Are
Generally Adequate, But Some Improvement Is Needed

This report presents the results of our review of the controls over the Internal Revenue Service's (IRS) Masterfile computing system. In summary, we found the security-sensitive system components and settings on the operating system of the Masterfile system to be adequate. However, there are several areas where improvements are needed to maintain a necessary level of security for the Masterfile system.

We recommended that the Chief, Information Technology Services, and the designated offices ensure that security documentation is current and complete, correct the identified non-compliant access controls, ensure that key system libraries are closely monitored and reviewed, and strengthen system password controls. Management agreed with our recommendations and developed appropriate corrective actions. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as Appendix V.

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

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Table of Contents

Results in Brief.....	Page 1
Objective and Scope.....	Page 2
Results.....	Page 4
Security Documentation for the Masterfile Mainframe System Is Incomplete and Outdated.....	Page 4
System-Level Access Controls Are Generally Adequate; However, Several Controls Are Not in Compliance with Internal Revenue Service Policies.....	Page 6
System Software Controls Are Generally Adequate; However, Several Key System Libraries Need to Be More Proactively Managed.....	Page 8
System Password Format Should Be Modified to Enhance User Authentication.....	Page 9
Summary of Recommendations.....	Page 11
Conclusion.....	Page 12
Appendix I – Additional Information on Weaknesses Identified.....	Page 13
Appendix II – Detailed Objective, Scope, and Methodology.....	Page 24
Appendix III – Major Contributors to This Report.....	Page 29
Appendix IV – Report Distribution List.....	Page 30
Appendix V – Management’s Response to the Draft Report.....	Page 31

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Results in Brief

The Masterfile computers are integral to the mission of the IRS and its collection activities.

This report presents the results of our review of the system software and system access controls of the Internal Revenue Service's (IRS) Masterfile mainframe computers residing at the Martinsburg Computing Center (MCC). The Masterfile computers are integral to the mission of the IRS and its collection activities by hosting the following systems:

- Masterfile: The IRS' database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
- Corporate Files On-Line (CFOL): CFOL provides nationwide access to information processed through any district/service center and posted to any of the Masterfiles.
- Information Returns Processing: Nationwide, all information returns, such as Forms 1099, are sent to the MCC where an extensive Information Returns Masterfile is maintained.

The Masterfile is a unique system in its importance to the IRS and the economy of the United States. In 1999, the IRS collected \$1.9 trillion in taxes, processed 130 million tax returns from individuals and businesses, and recorded 234 million payments. These numbers are projected to grow throughout the foreseeable future. In addition, at the time of our review there were over 1,300 users with system-level access to the Masterfile system, which includes users such as programmers, operators, and database administrators. Of these, 14 users had been granted privileged levels of access to the system, which enable the users to either issue all security commands, access protected resources, or modify audit settings. Due to its importance, the IRS must pay careful attention that the Masterfile system complies with Federal Government and IRS prescribed

Due to its importance to the IRS and the nation, the IRS must pay careful attention that the Masterfile system complies with Federal Government and IRS prescribed policies and procedures.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

policies and procedures to ensure that the system is adequately secured.

In general, we found the security-sensitive system components and settings for the Masterfile operating system¹ to be adequate. However, we identified weaknesses with the security documentation, systems software management, and several logical access controls, that require management's attention to ensure the security of the Masterfile mainframe system. The identified conditions indicate that the Masterfile mainframe system is potentially vulnerable to unauthorized access and, as a result, sensitive data maintained on the system could be improperly used, changed, or destroyed.

Objective and Scope

The overall objective of this review was to evaluate the system software and system access controls of the Masterfile mainframe computers.

The overall objective of this review was to evaluate the system software and system access controls of the Masterfile mainframe computers and assess the IRS' progress in meeting appropriate security requirements for these mainframes.

During this review we determined whether:

- Controls over Masterfile computer system resources provided reasonable assurance that data files, application programs, and computer-based facilities and equipment were protected against unauthorized modification, disclosure, loss, or impairment.
- Controls over access to and modification of Masterfile computer system software provided reasonable assurance that operating system-based controls are not vulnerable to intentional or accidental changes.

¹ The Masterfile system runs the OS/390 operating system, which is IBM's standard operating system for its mainframe computers.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

- Pertinent security documents were completed and effective security procedures were implemented.

The Treasury Inspector General for Tax Administration (TIGTA) controlled this review and received assistance from the Information Technology staff of the General Accounting Office (GAO) in completing the technical aspects of this review. This assistance included the use of the GAO's computer lab to perform some of our audit tests.

To assist in our review of controls over the access to and modification of the computer system software on the Masterfile system, we used Computer Associate's audit software, CA-Examine. CA-Examine helps identify control and security exposures in OS/390 operating systems. We used this product to analyze the controls governing critical operating system programs and settings.

This review addresses the IRS' strategy of promoting effective asset and information stewardship by evaluating the system-level security of the Masterfile system. This strategy includes several security-related goals, including the review of the state of IRS security and a focus on providing solutions to identified weaknesses.

Audit work was performed on-site at the MCC and in the IRS' National Headquarters in the offices of the Chief, Information Technology Services, from July 2000 to March 2001. This audit was performed in accordance with *Government Auditing Standards*.

Detailed information on findings identified in this report and specific recommendations are presented in Appendix I. Details of our audit objective, scope, and methodology are presented in Appendix II. Major contributors to this report are listed in Appendix III.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Results

In general, we found the controls over sensitive system components and settings for the Masterfile operating system to be adequate.

In general, we found the controls over sensitive system components and settings for the Masterfile operating system to be adequate. Our review of the system software components found that the settings for the high-risk components² are generally appropriate. In addition, our review of logical access controls found that adequate controls are in place to identify and authenticate users, restrict access to appropriate programs and information, and monitor and review audit trails of user activity.

There are several areas, however, where improvements are needed to maintain a necessary level of security for the Masterfile system. Such improvements are needed because any control weaknesses found on the Masterfile system, even minor ones, are amplified due to the importance of this system to the Federal Government and the nation's economy.

Security Documentation for the Masterfile Mainframe System Is Incomplete and Outdated

The foundation for ensuring adequate protection for this, or any system, is adequate security documentation.

In a system that is as essential to the nation's tax processing capability as the Masterfile system, it is of utmost importance that it be adequately protected from all preventable security breaches. The foundation for ensuring adequate protection for this, or any system, is adequate security documentation. Without adequate documentation, security controls may be inadequate and/or inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and data.

² High-risk components refers to system software that, if compromised, would likely result in the compromise of the integrity of the entire system.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Our review identified several security policies in place for the Masterfile. Specifically:

- A Computer Security Plan for the Masterfile system.
- A Risk Analysis of the Masterfile system.
- An IRS-wide Law Enforcement Manual (LEM) specifying security standards for OS/390 systems.
- Several MCC security policies to supplement the above policies.

Our review of the security documentation for the Masterfile system identified that several of the documents do not meet the minimum standards set forth in Federal and IRS guidelines, including the Office of Management and Budget's (OMB) Circular A-130, "Management of Federal Information Resources," the Internal Revenue Manual (IRM), and the recently released Federal Information Technology Security Assessment Framework. Specifically, both the Computer Security Plan and Risk Analysis were completed in 1995. OMB Circular A-130 and IRS guidelines require these documents to be updated at least every 3 years. Consequently, they do not reflect changes to the system or its environment, including upgrades in the mainframe hardware and changes in the location of personnel supporting the Masterfile system. In addition, while the Computer Security Plan includes all of the section titles required by OMB Circular A-130 and the IRM, the necessary detailed information as prescribed by these standards was not included.

For example, the Computer Security Plan is required by Circular A-130 to include personnel controls regarding initial and periodic screening of individuals "authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause." On the Masterfile system, such authorization includes users granted system-level privileges. However, the Computer Security Plan does not include this requirement. Consequently, only 5 of the 11 users with this level of

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Without current and complete security documentation, the IRS cannot ensure that all risks and vulnerabilities to its computer systems have been identified, assessed, and adequately mitigated.

access had background investigations completed in the last 5 years, with only 1 user having an investigation completed in the last 3 years. The remaining users were last screened between 10 and 25 years ago. By not conducting periodic background investigations on users with system-level privileges, the IRS runs the risk of failing to detect continuing unauthorized employee actions by individuals with sensitive access to one of the most important information systems in the IRS.

These documents form the foundation of the security program for the Masterfile system, which includes the implementation, administration, and oversight of security for the system. If the information contained in these documents is not current and complete, the security program for the Masterfile system may not have the information needed to adequately secure the system. As a result, the IRS cannot ensure that all risks and vulnerabilities to its computer systems have been identified, assessed, and adequately mitigated.

We were informed by MCC personnel that they had completed the required revisions to the documentation and were waiting further action from the Certification Office. In our communications with the Office of Security Evaluation and Oversight (SEO), we were unable to obtain a current schedule for updating the Masterfile security documentation. In addition, we were unable to determine why a significant amount of time had passed since this documentation was last updated.

System-Level Access Controls Are Generally Adequate; However, Several Controls Are Not in Compliance with Internal Revenue Service Policies

Access controls should provide reasonable assurance that a computer system and its application programs and data are protected against unauthorized modification and disclosure. Inadequate access controls diminish the reliability of computerized data and increase the risk of unauthorized modification, disclosure, loss, or impairment of data. On the Masterfile system, logical access controls are implemented through the Resource

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Our review of logical access controls found that, in general, adequate controls are in place to identify and authenticate users, restrict access to appropriate programs and information, and monitor and review audit trails of user activity.

Access Control Facility (RACF). The IRS has established standards for the use of the RACF through the RACF LEM. These standards must be followed diligently in order to maintain a strong control environment that prevents unauthorized access and compromise of the system.

Our review of logical access controls found that, in general, adequate controls are in place to identify and authenticate users, restrict access to appropriate programs and information, and monitor and review audit trails of user activity. However, several instances were identified where controls on the Masterfile system were not in compliance with controls specified in the RACF LEM. Specifically, we identified instances where controls were non-compliant for assigning sensitive privileges to users and groups of users, timely removal of unnecessary access, and implementing the system-level auditing facility for two system resources.

The MCC staff advised us that some of the instances identified above deviated from the LEM requirements because of periodic peaks in their workload, which caused the MCC staff to postpone all but crucial processes. For other instances, the MCC staff believes that the deviations are necessary so that the users can perform their assigned responsibilities. However, waivers for deviations from the LEM had not been submitted for approval to the SEO, as required by the LEM. In addition, the lack of a security review in the year 2000 contributed in part to non-compliance with the controls. In the past, the SEO has conducted such reviews; however, none were conducted at the MCC during the year 2000.

(b)(2),(b)(7)(E)

The MCC staff disagrees with the LEM requirement to [REDACTED]. In their view, implementing such a requirement would generate an excessive amount of unnecessary system audit trail records. To support their position, the MCC technical staff cited IBM documentation which states that, as a general rule, [REDACTED].

(b)(2),(b)(7)(E)

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

(b)(2),(b)(7)(E) [REDACTED] The SEO, however, has informed us that they do not plan to remove this requirement from the LEM. Although we believe a waiver should be submitted, we were unable to obtain sufficient information to determine from a technical viewpoint whether it should be granted.

**System Software Controls Are Generally Adequate;
However, Several Key System Libraries Need to Be
More Proactively Managed**

System software is a set of programs designed to operate and control the processing activities of computer equipment. Programs on OS/390 operating systems are organized into libraries, through which access to the programs is controlled. Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Inadequate controls in this area could lead to unauthorized access and circumvention of security controls to read, modify, or delete critical or sensitive information and programs. In our assessment of the controls over the system software configuration on the Masterfile system, we found the settings for the high-risk components of the system software to be generally appropriate, with two exceptions. In addition, we identified 49 users with privileged access to many key system libraries and determined that, based on their job responsibilities, this access is appropriate.

With two exceptions, our review found the settings for the high-risk components of the system software to be generally appropriate.

The exceptions identified were weaknesses in several key system libraries. Specifically, we found the following:

- There are weaknesses with two key system libraries that, in the absence of compensating controls, would present a significant security risk to the system by creating the opportunity for an unauthorized program to gain privileged access to the system. For these libraries, there are compensating controls in place to prevent this situation from occurring.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

However, it is possible that, in the future, other system software libraries might be vulnerable if compensating controls are not in place.

- There are programs with identical names that exist within numerous key system libraries. Our review of all 172 key system libraries identified 101 libraries that contained instances of identically named programs. IBM documentation explains that the existence of programs with the same name could lead to the accidental or deliberate use of the wrong programs and the possible introduction of a system integrity exposure.

These two weaknesses resulted from the lack of specific policies or guidance on managing the content of these key system libraries. The IRM does not include policies or guidance on maintaining system software for the Masterfile system. However, the IRM assigns the responsibility for developing overall Masterfile processing procedures to the MCC. While the MCC has local procedures in place for managing the installation and configuration of system software, there are no specific procedures in place for managing the contents of these key libraries. The documentation accompanying the CA-Examine tool recommends that authorized key system libraries should be closely monitored for frequency of updates due to the powerful access granted to these libraries.

System Password Format Should Be Modified to Enhance User Authentication

User access to information systems is typically controlled through identification and authentication of the user. Identification is the process of distinguishing one user from all others, usually through the use of user identifiers (UserID). Authentication is the process for determining whether users are who they say they are. The most widely used method of authentication is through the use of passwords. Passwords can be structured at varying levels of complexity to increase the

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Our review of password controls on the Masterfile system determined that the password settings for the system appear adequate; however, the password format can be improved.

level of difficulty in compromising passwords and user authenticity.

Our review of the password controls on the Masterfile system determined that the password settings for the system appear adequate and compliant with IRS and Federal Government requirements for password length. Although the password length is technically in compliance with these requirements, it has been given a structure that limits the protection offered by a password of its length. For example, the password format for the Masterfile system does not prevent users from creating passwords that closely mirror the format of their UserID or including easily guessed user information (e.g., meaningful dates). In addition, the Masterfile system password format makes it easier for passwords not to conform to IRM password standards, such as requirements not to use obvious combinations of letters and numbers or personal information in user passwords. The password format also results in significantly fewer possible password combinations (6.7 million) than the format required for other similar mainframe systems at the MCC (119 million). Consequently, this format could allow an internal attacker to more easily guess an authorized system user's password. Once the attacker obtains a user's password, he or she can then execute all the system commands that are ascribed to that user.

We also found that the password format for the Masterfile mainframe system, as well as other MCC mainframes, is posted on the MCC Intranet website. This website is accessible to all IRS employees and authorized contractors. The IRM, while not specifically prohibiting this situation, does require that a system should block out any demonstration of password length. While passwords are in fact blocked out on the Masterfile system, the existence of the password structure on the Intranet site circumvents this control by making the password length available not only to users of the Masterfile system but anyone with access to the IRS Intranet.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Summary of Recommendations

The specific recommendations for this report are presented in Appendix I. In summary, to correct the weaknesses identified in the report, the Chief, Information Technology Services and the designated offices should:

- Ensure that security documentation for the Masterfile system is current and complete, including specific requirements for background investigations of users with sensitive system access.
- Correct the identified non-compliant access controls or obtain approval to waive LEM requirements, and coordinate periodic reviews of the Masterfile system to ensure access controls are compliant with the LEM.
- Ensure that authorized key system libraries are closely monitored by systems programmers and reviewed to prevent duplication of programs in these libraries.
- Remove system password formats from the MCC Intranet and increase the complexity of the password format on the Masterfile system.

Management's Response: IRS management stated that the Masterfile security documentation is now complete, except for the Security, Test and Evaluation test plan. IRS management also stated that steps have been taken or are in process to correct the non-compliant access controls. In certain instances, waivers for the LEM requirements are being developed. Programs are being developed to notify programming personnel of duplicate key system library programs. IRS management has removed the system password formats from the Intranet and will study increasing the complexity of system passwords.

Management's complete response has been included as Appendix V to this report.

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Conclusion

The Masterfile system is critically important to the nation's ability to collect taxes and therefore must remain at the highest levels of security.

The IRS' Masterfile system is one of the most important systems in the IRS and is critically important to the nation's ability to collect taxes. Consequently, the system must be adequately secured and in compliance with appropriate Federal and agency guidelines to prevent the opportunity for minor weaknesses to escalate into system compromises.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Appendix I

Additional Information on Weaknesses Identified

The Masterfile mainframe system is integral to the mission of the Internal Revenue Service (IRS) and the focal point of the nation's tax processing capability. In 1999, the IRS collected \$1.9 trillion in taxes, processed 130 million tax returns from individuals and businesses, and recorded 234 million payments. These numbers are projected to grow throughout the foreseeable future. In addition, at the time of our review there were over 1,300 users with system-level access to the Masterfile system, which includes users such as programmers, operators, and database administrators. Of these, 14 users had been granted system-level attributes, or privileged levels of access to the system, which enables these users to either issue all security commands, access protected resources, or modify audit settings. Any control weaknesses found on the system, even minor ones, are amplified due to the importance of this system to the Federal Government and the nation's economy.

Security Documentation for the Masterfile Mainframe System Is Incomplete and Outdated

In a system that is as essential to the nation's tax processing capability as the Masterfile system, it is of utmost importance that it be adequately protected from all preventable security breaches. The foundation for ensuring adequate protection for this, or any system, is adequate security documentation. Without adequate documentation, security controls may be inadequate and/or inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and data.

Our review identified several security policies in place for the Masterfile, including:

- A Computer Security Plan for the Masterfile system.
- A Risk Analysis of the Masterfile system.
- An IRS-wide Law Enforcement Manual (LEM) specifying security standards for OS/390 systems.¹
- Several Martinsburg Computing Center (MCC) security policies to supplement the above policies.

¹ The Masterfile system runs the OS/390 operating system, which is IBM's standard operating system for its mainframe computers.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Our review of the security documentation for the Masterfile system identified that several of the documents do not meet the minimum standards set forth in Federal and IRS guidelines. Specifically, the following standards apply:

- In November 2000, the Chief Information Officers Council released a new framework for managing risks to computer systems. This framework provides the Federal Government a consistent approach in conducting annual program reviews required by the Government Information Security Reform Act. To meet the minimum requirements of the first level of the new framework, the computer system must have “a formally, up-to-date documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness.”
- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” states that security controls in each system should be reviewed “when significant modifications are made to the system, but at least every 3 years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system.”
- The IRS’ Internal Revenue Manual (IRM) states “The security plan must be reviewed annually.” If such a review is not completed, the system could become vulnerable to significant unidentified risks that place the integrity of the system in question.

We found that two important security documents did not meet these standards as a result of being significantly out of date and missing some required information. Specifically:

- Computer Security Plan: Our review of the security documentation for the Masterfile system determined that the Computer Security Plan for the system was completed in mid-to-late 1995. (An approximation of the date was necessary since the Computer Security Plan was not dated.) While the Computer Security Plan includes all of the headings found in OMB Circular A-130, the IRM, and National Institute of Standards and Technology requirements, the information under each heading does not meet the requirements prescribed by the standards. These headings address system identification, system function and purpose, sensitivity of information handled by the system, status of security activities and control measures, rules of behavior, training, personnel controls, incident response capability, continuity of support, technical security, and system interconnection.
- Risk Analysis: The Risk Analysis of the Masterfile system, dated September 1995, was completed to fulfill the requirements of OMB Circular A-130 and the requirements for System Security Certification. The Masterfile system was certified in November 1996. Our review of the Risk Analysis identified that several areas of the document are out-of-date and do not reflect significant changes made to the system since it was certified. For example, at the time of the Risk Analysis, the

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Masterfile system was hosted on two Hitachi mainframe computers. However, since then, the Masterfile system has migrated to IBM 9672 mainframes as well as more recent versions of the OS/390 operating system. In addition, there have been several changes made to the physical location of much of the system equipment.

Specifically, since 1995, both MCC personnel and a significant portion of the IRS' Information Technology Services personnel have been centralized into new buildings in Martinsburg, West Virginia, and New Carrollton, Maryland, respectively. The Risk Analysis does not reflect these changes.

Without current and complete security documentation, the IRS cannot ensure that all risks and vulnerabilities to its computer systems have been identified and adequately mitigated. For example, the Computer Security Plan is required by Circular A-130 to include personnel controls regarding initial and periodic screening of individuals "authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause." On the Masterfile system, such authorization includes users granted system-level attributes (system-SPECIAL, etc.). However, the Computer Security Plan does not include this requirement. Consequently, only 5 of the 11 users with this level of access had background investigations completed in the last 5 years, with only 1 user having an investigation completed in the last 3 years. The remaining users were last screened between 10 and 25 years ago. By not conducting periodic background investigations on sensitive system users, the IRS runs the risk of failing to detect improper employee actions by individuals with sensitive access to one of the most important information systems in the IRS.

We were informed by MCC personnel that they had completed the required revisions to the documentation and were waiting further action from the Certification Office. In our communications with the Office of Security Evaluation and Oversight (SEO), we requested a current schedule for updating the Masterfile security documentation and the reason for the delay, but none was provided.

Recommendations

1. The Chief, Information Technology Services, should ensure the security documentation for the Masterfile mainframe system is reviewed and made current and complete, according to existing Federal standards.

Management's Response: All security re-certification documentation is complete for the Masterfile mainframe system. The final step in the process is the completion of the Security, Test and Evaluation test plan.

2. The Chief, Information Technology Services, should ensure that the Computer Security Plan for the Masterfile system includes specific requirements for periodic background investigations of individuals with sensitive system access of no less than

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

every 5 years. These individuals should include, at a minimum, users with system-level attributes.

Management's Response: A management team composed of representatives from the MCC, the SEO, and Personnel Security will re-evaluate the Computer Security Plan and associated investigative requirements for sensitive system access.

System-Level Access Controls Are Generally Adequate; However, Several Controls Are Not in Compliance with Internal Revenue Service Policies

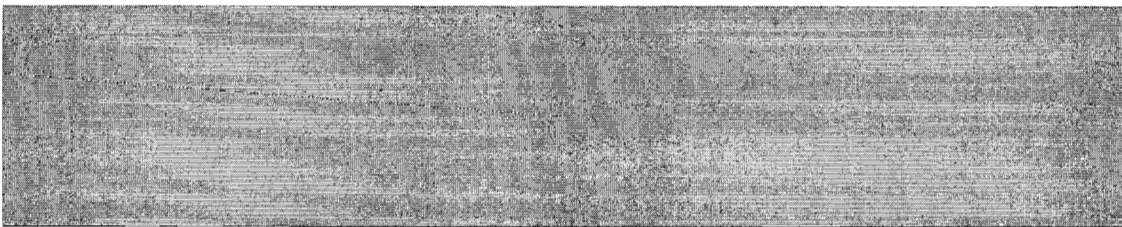
Access controls should provide reasonable assurance that a computer system and its application programs and data are protected against unauthorized modification and disclosure. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. The scope of our review included an assessment of logical access controls, or controls implemented through computer hardware and software to prevent unauthorized access to a system.

On the Masterfile system, logical access controls are implemented through the Resource Access Control Facility (RACF). Our review of logical access controls found that, in general, adequate controls are in place to identify and authenticate users, restrict access to appropriate programs and information, and monitor and review audit trails of user activity.

The IRS' RACF LEM establishes a set of standards that will create and maintain a strong access control environment for systems using the RACF. These standards must be followed diligently in order to maintain a strong control environment that prevents unauthorized access and compromise of the system.

Our review of the logical access controls for the Masterfile system identified several instances where controls were not in compliance with the RACF LEM. Specifically:

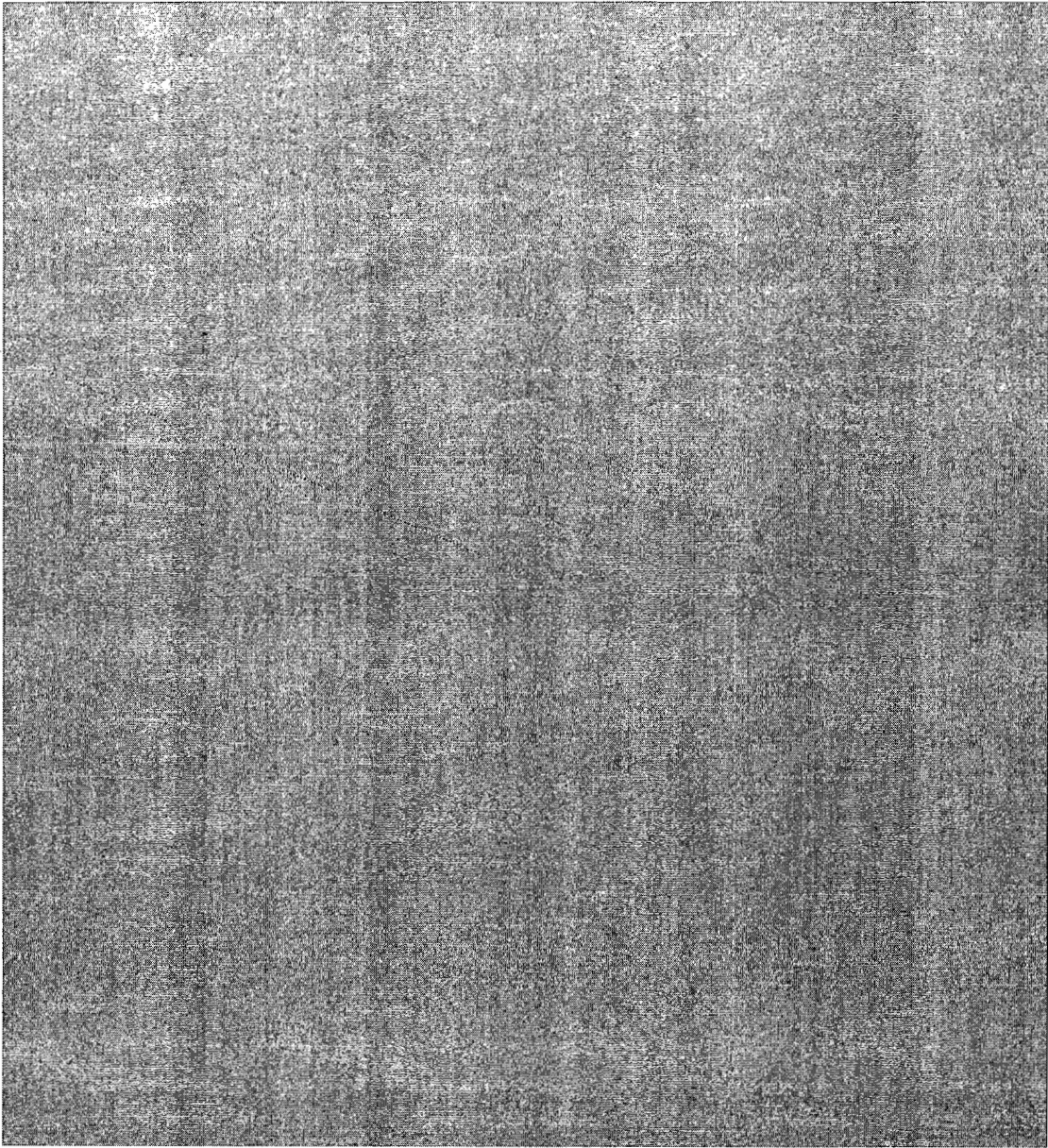
(b)(2),(b)(7)(E)



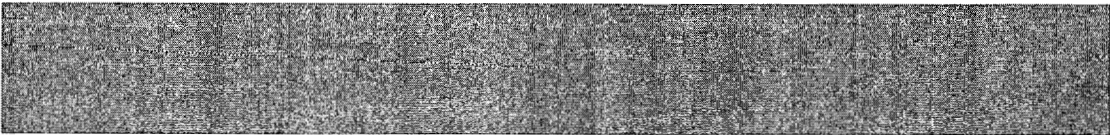
(b)(2),(b)(7)(E)

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

(b)(2),(b)(7)(E)




(b)(2),(b)(7)(E)



**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**


(b)(2),(b)(7)(E)



Through discussions with MCC Security staff, it was acknowledged that for some of the instances identified above the staff does not follow the LEM requirements because of periodic peaks in their workload, which caused the MCC staff to postpone all but crucial processes. For other instances, the MCC staff believes that the deviations are necessary in order for the users to perform their assigned responsibilities. However, waivers for deviations from the LEM had not been submitted for approval to the SEO, as required by the LEM.

In addition, the lack of a security review of the Masterfile system during 2000 contributed in part to the identified non-compliant controls. In the past, the SEO has conducted periodic security reviews, usually twice a year, at IRS facilities. These reviews included testing of both physical and logical controls over systems at IRS facilities.

(b)(2),(b)(7)(E)



create a significant amount of unnecessary Systems Management Facility records, which must be handled by the Security Analysts for the system and would create an unnecessary burden. To support their position, the MCC technical staff cited the IBM RACF Security Auditor's Guide, which states that as a general rule accesses to most general resources should not be audited. The SEO, however, has informed us that they do not plan to remove this requirement from the LEM. During the review we were unable to obtain sufficient information to determine whether a waiver of this requirement is warranted.

Recommendations

3. The Director, MCC, should correct the identified instances of non-compliance with the LEM on the Masterfile system or obtain approval to deviate from the LEM from the SEO.

Management's Response:

- Over the past several years, the MCC has taken steps to considerably reduce the number of staff having multiple group-level attributes.
- The System Auditor attribute was removed from the Security Specialist's UserID after completion of the assigned tasks.
- The unique nature of the work periodically necessitates deviating from the LEM. Whenever this occurs, the MCC Security and Disclosure Branch will prepare and

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

submit a deviation request from the RACF LEM standard. The deviation request will include a justification for the deviation, including the steps to be taken to mitigate risks.

(b)(2),(b)(7)(E)

- The MCC Security and Disclosure Branch will schedule and monitor regular reviews of UserIDs that are [REDACTED] in order to delete them from the system. The reviews will support proper system maintenance and assist in ensuring the system complies with the LEM.

(b)(2),(b)(7)(E)

[REDACTED]

performance problem arises as the result of this capability being activated, the MCC Security and Disclosure Branch will prepare and submit a deviation request from the RACF LEM standard.

- The Director, MCC, reviewed applicable system definitions and determined that all data are now current.

(b)(2),(b)(7)(E)

[REDACTED]

Management's Response: The MCC Security and Disclosure Branch will prepare and submit a deviation request from the RACF LEM standard. The request will include a justification for the deviation, including the steps to be taken to mitigate risks.

(b)(2),(b)(7)(E)

[REDACTED]

in compliance with the IRS' RACF LEM.

Management's Response: An onsite review of the MCC and the Masterfile system was performed by the SEO during the week of April 23 through April 27, 2001. In addition, SEO analysts are gaining remote access to the Masterfile to conduct periodic, unannounced online reviews of the Masterfile system to ensure that its access controls are in compliance with the RACF LEM and other requirements. These reviews will be separate from the onsite reviews [REDACTED] in compliance with the RACF LEM.

(b)(2),(b)(7)(E)

System Software Controls Are Generally Adequate; However, Several Key System Libraries Need to Be More Proactively Managed

System software is a set of programs designed to operate and control the processing activities of computer equipment. Programs on OS/390 operating systems are organized into libraries, through which access to the programs is controlled. Controls over access to and modification of system software are essential in providing reasonable assurance that

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

operating system-based security controls are not compromised and that the system will not be impaired. Inadequate controls in this area could lead to unauthorized access and circumvention of security controls to read, modify, or delete critical or sensitive information and programs.

In our assessment of the controls over the system software configuration on the Masterfile system, we found the settings for the high-risk components,⁴ including system exits, supervisor calls, and input/output appendages, are generally appropriate. In addition, we identified 49 users with privileged access, including UPDATE or ALTER access, to Authorized Program Facility (APF) libraries. We determined that, based on their job responsibilities, this access is appropriate. However, our review identified two weaknesses with the APF libraries that, in the absence of compensating controls, would present a significant security risk to the system.

Specifically, our review of the APF-authorized libraries identified two libraries that were not located on the volume specified in the APF list. Such a discrepancy is identified by the system when booted, or initial program load (IPL), but not necessarily brought to the attention of appropriate personnel. In the absence of compensating controls, this would present a significant security risk by creating the opportunity for an unauthorized program to become APF authorized by using the same name and volume specified on the APF list. As a result, it would be possible for such a program to circumvent all standard OS/390 security controls, including access to secured data. Our review of the Masterfile system identified compensating controls, through RACF profiles for these libraries, to prevent this situation from occurring. However, it is possible that other system software libraries in the future might be left vulnerable if, for instance, the profiles governing these libraries are less restrictive and permit widespread access to modify the libraries.

We also found that identically named programs exist within APF libraries. IBM guidelines state that installations using APF authorization must control which programs are stored in authorized libraries and ensure that no two programs with the same name exist across the set of authorized libraries. However, we found that 101 of all 172 APF libraries reviewed contained instances of identically-named programs. Collectively, over 18,000 instances of duplication exist 2 or more times within these 101 APF-authorized libraries. The existence of programs with the same name could lead to the accidental or deliberate use of the wrong programs and the possible introduction of a system integrity exposure.

⁴ High-risk components refers to system software that, if compromised, would likely result in the compromise of the integrity of the entire system.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

These two weaknesses resulted from the lack of specific policies or guidance on managing the content of these key system libraries. Our review of the IRM did not identify any policy or guidance on maintaining system software or the APF list. However, the IRM assigns responsibility for developing overall Masterfile processing procedures to the MCC. While the MCC has local procedures in place for managing the installation and configuration of system software, there are no specific procedures in place for managing the contents of the APF list or members of APF libraries. The documentation accompanying the CA-Examine tool recommends that APF libraries be closely monitored for frequency of updates due to the powerful access granted to these libraries.

Recommendations

6. The Director, MCC, should ensure that the APF libraries are closely monitored, including devising a control mechanism to alert systems programmers at IPL of APF-authorized libraries that are not on volumes specified in the APF list.

Management's Response: The MCC will write a utility program that will read the Progxx members of Parmlib and report any discrepancies. This will be a ControlM job that will execute at least once a week. Notification of any discrepancies will be sent to various systems programmers and managers.

7. The Director, MCC, should develop procedures for periodically reviewing the contents of APF libraries to ensure that instances of duplicate programs are reduced.

Management's Response: The MCC implemented procedures for a system monitoring program to periodically produce a report of the duplicate modules. This report is being reviewed to ensure there are no unnecessary duplication of modules.

System Password Format Should Be Modified to Enhance User Authentication

User access to information systems is typically controlled through identification and authentication of the user. Identification is the process of distinguishing one user from all others, usually through the use of UserIDs. Authentication is the process for determining whether users are who they say they are. The most widely used method of authentication is through the use of passwords. Passwords can be structured at varying levels of complexity to increase the level of difficulty in compromising passwords and user authenticity.

Our review of the password controls on the Masterfile system determined that the password settings for the system appear adequate. The parameters for revocation of inactive passwords and mandatory password changes are appropriate. In addition, the password length is in compliance with IRS and Federal Government requirements.

Although the password length is technically in compliance with these requirements, it has been given a structure that limits the protection offered by a password of its length. As a

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

result, the password format for the Masterfile system is not sufficiently complex and could allow an internal attacker to more easily guess an authorized system user's password. Once the attacker obtains a user's password, he or she can then execute all the system commands that are ascribed to that user.

Specifically, the password format on the Masterfile system is "AANNNN," where A is an alpha character and N is a numeric character. This format is problematic for the following reasons:

- The format too closely mirrors the format of the UserIDs. Therefore, users may likely use the UserID in the password.
- The format lends itself to easily guessed passwords, such as user initials and birthdate, last four digits of the user's social security number (SSN), or some other significant number.

Other IRS mainframe computers running the OS/390 operating system and using the RACF have more complex password formats. For example, the ICS/ACS/PRINT (Integrated Collection System/Automated Collection System/Printer Replacement to Integrate New Tools) system, another OS/390-based mainframe system at the MCC, uses a password format comprised of mostly alpha characters. However, one numeric character is used and is placed in the middle of the password. For the Masterfile system, such a structure would increase password complexity by preventing users from mirroring their UserID as well as using meaningful dates. Such a format would also increase the number of possible password combinations from 6.7 million to 119 million passwords, significantly decreasing the likelihood of password compromise.

In addition, the Masterfile system password format makes it easier for passwords to not conform with standards specified in the IRM:

- Passwords should not be comprised of obvious combination of letters and numbers (e.g., first names, last names, initials, birth dates, or user identifications spelled backwards).
- Passwords should not be created that are related to personal identity, history, or environment.
- The system shall provide a means for ensuring the complexity of user-entered passwords.

In addition, the required password format for the Masterfile mainframe system is posted on the MCC Intranet website. This website is accessible to all IRS employees and authorized contractors. The IRM, while not specifically prohibiting this situation, does require that a system should block out any demonstration of password length. While passwords are in fact blocked out on the Masterfile system, the existence of the password structure on the Intranet site circumvents this control by making the password length

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

available not only to users of the Masterfile system but anyone with access to the IRS Intranet.

Recommendations

8. The Director, MCC, should ensure that system password formats are removed from the MCC Intranet.

Management's Response: System password formats were removed from the Intranet.

9. The Director, MCC, should restructure the password format for the Masterfile system to increase the complexity of the passwords, thus making them more difficult to guess or crack.

Management's Response: A management team led by the SEO, and assisted by the MCC, will assess the adequacy of existing passwords and conduct a feasibility study for restructuring password formats.

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

Appendix II

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the system software and system access controls in the Masterfile system and assess the Internal Revenue Service's (IRS) progress in meeting appropriate security requirements for this system. This review included evaluation of the general control environments over the production Masterfile mainframe systems at the Martinsburg Computing Center. The scope of this review encompassed an evaluation of system policies as they relate to the Masterfile system, system software controls, and access controls at the system level. We reviewed identification and authentication controls, discretionary access controls, and system audit trail policies.

To accomplish these objectives, we:

- I. Obtained background information on the Masterfile system to determine how critical the system is to the IRS' tax processing system by:
 - A. Reviewing system manuals and other documentation to gain an understanding of the system.
 - B. Identifying the number of users with access to applications residing on the Masterfile mainframe as well as with direct access to the system.
 - C. Identifying the volume of transactions and the dollar amount being processed by the Masterfile mainframes on an annual basis.
 - D. Identifying the number of systems that can request database extracts or other information from the system.
- II. Assessed the Masterfile system security policies to ensure a risk assessment policy was in place and effective security procedures had been implemented by:
 - A. Researching current topics in the areas of mainframe and network security, including recent security breaches and corresponding solutions to identify potential risk areas.
 - B. Determining if a current risk assessment exists for the Masterfile and reviewing it to ensure that vulnerabilities were identified and mitigated.
 - C. Determining if a current security plan for the Masterfile existed and reviewing it to ensure it covered all major components and included topics prescribed by the Office of Management and Budget's Circular A-130, including:

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

- Rules of the system/Application rules.
 - Training/Specialized training.
 - Personnel controls/Personnel security.
 - Incident response capability.
 - Continuity of support/Contingency planning.
 - Technical security/Technical controls.
 - System interconnection/Information sharing.
- III. Determined whether controls over access to and modification of system software provided reasonable assurance that operating system-based controls were not compromised and that the system would not be impaired by:
- A. Determining that all access paths through the system software had been identified and controls implemented to prevent or detect access for all paths. Specifically, we:
1. Obtained a list of vendor-supplied software and determined if any of these products had known deficiencies that adversely affect system integrity (e.g., using system integrity statement provided by vendor).
 2. Reviewed the operating system to determine if it had been configured to prevent circumvention of the security software and application controls. We used CA-Examine to analyze the software and hardware environment of the Masterfile OS/390 system.
 3. Determined that vendor-supplied default logon identifiers and passwords had been disabled.
 4. Determined if remote access to the system master console was restricted.
- B. Determining the policies and techniques that had been implemented for using and monitoring use of system utilities. We determined if:
1. Policies and procedures for using and monitoring use of system software utilities existed and were up-to-date.
 2. Responsibilities for using sensitive system utilities had been clearly defined and were understood by systems programmers.
 3. Responsibilities for monitoring the use of system utilities were defined and understood by technical management.
 4. The use of sensitive system utilities was logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).
- C. Determining whether inappropriate or unusual activity was investigated and appropriate actions taken by determining if:

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

1. The use of privileged system software and utilities was reviewed by technical management.
 2. Inappropriate or unusual activity in using utilities was investigated.
 3. Systems programmers' activities were monitored and reviewed.
 4. Management reviews were performed to determine that control techniques for monitoring use of sensitive system software were functioning as intended and that the control techniques in place were maintaining risks within acceptable levels (e.g., periodic risk assessments).
- D. Determining if system software changes were authorized, tested, and approved before implementation. We determined whether:
1. Policies and procedures existed and were up-to-date for identifying, selecting, installing, and modifying system software.
 2. Procedures existed for identifying and documenting system software problems. These procedures normally include using a log to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.
 3. New system software versions or products and modifications to existing system software received proper authorization and were supported by a change request document.
 4. New system software versions or products and modifications to existing system software were tested and the test results were approved before implementation.
 5. Procedures existed for controlling emergency changes.
- E. Evaluating the installation of system software by determining if:
1. Installation of system software was scheduled to minimize the impact on data processing and advance notice was given to system users.
 2. Migration of tested and approved system software to production use was performed by an independent library control group.
 3. Installation of all system software was logged to establish an audit trail and reviewed by data center management.
 4. Vendor-supplied system software was supported by the vendor.
 5. All system software was current and had current and complete documentation.
- IV. Determined whether controls over system resources provided reasonable assurance that data files, application programs, and computer-based facilities and equipment were protected against unauthorized modification, disclosure, loss, or impairment by:

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

- A. Determining if resource classifications and related criteria had been established.
- B. Determining if resource classifications were based on risk assessments and classifications were documented and approved by an appropriate senior official and were periodically reviewed.
- C. Determining whether authorized users had been identified and their accesses authorized. We determined whether:
 - 1. Policies and procedures for restricting access existed and were up-to-date.
 - 2. Access authorizations were documented on standard forms and maintained on file, approved by senior managers, and securely transferred to security managers.
 - 3. Access authorization listings were periodically reviewed.
 - 4. Access to system software was restricted to a limited number of personnel, corresponding to job responsibilities; application programmers and computer operators were specifically prohibited from accessing system software; and update access was generally limited to primary and backup systems programmers.
 - 5. The number of users who can dial into the system from remote locations was limited and justification for such access was documented and approved by owners.
 - 6. Security managers reviewed access authorizations and discussed any questionable authorizations with resource owners.
 - 7. All changes to security profiles by security managers were automatically logged and periodically reviewed by management independent of the security function and unusual activity was investigated.
 - 8. Security was notified immediately when system users were terminated or transferred.
- D. Identifying that emergency and temporary access authorization was controlled.
- E. Determining how the resource owners determined the disposition and sharing of data. We determined whether:
 - 1. Standard forms were used to document approval for archiving, deleting, or sharing data files.
 - 2. Prior to sharing data or programs with other entities, agreements were documented regarding how those files were to be protected.

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

- F. Evaluating the implementation of logical access controls by determining if:
1. Passwords, tokens, or other devices were used to identify and authenticate users.
 2. An analysis of the logical access paths was performed whenever changes to the system were made.
 3. Logical controls were in place to restrict access to the data files and software programs.
 4. Security software was used to restrict access by evaluating whether:
 - Security administration personnel set parameters of security software to provide access as authorized and restrict access that had not been authorized. These parameters include access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files. We used the IBM Security Server to perform this work.
 - Access to security software was restricted to security administrators only.
 - Inactive users' accounts were monitored and removed when not needed.
- G. Determining if audit trails were maintained, identifying that all activity involving access to and modifications of sensitive or critical files was logged. We determined whether:
1. Actual or attempted unauthorized, unusual, or sensitive access was monitored.
 2. Suspicious access activity was investigated and appropriate action taken.

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Appendix III

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
Myron Gulley, Senior Auditor
Michael Howard, Senior Auditor
Van Warmke, Senior Auditor
Kim McManis, Auditor

General Accounting Office Contributors:

Gregory Wilshusen, Assistant Director
Ed Glagola, Assistant Director
David Hayes, Assistant Director
Ronald Parker, Senior EDP Auditor
Denise Fitzpatrick, Information Systems Analyst

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Appendix IV

Report Distribution List

Commissioner N:C
Chief, Information Technology Services M:I
Director, Corporate Computing M:I:E
Director, Martinsburg Computing Center M:I:E:MC
Director, Office of Security M:S
Director, Strategic Planning and Client Services M:SP
Deputy Chief Financial Officer, Department of the Treasury

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

Appendix V

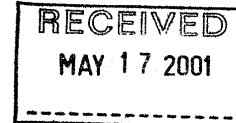
Management's Response to the Draft Report



DEPUTY COMMISSIONER

LIMITED OFFICIAL USE


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



May 15, 2001

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:


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

SUBJECT:

Response to Draft Report – Controls Over the Masterfile
System Are Generally Adequate, But Some Improvement Is
Needed

Thank you for the opportunity to review and comment on your draft report and recommendations concerning our Masterfile mainframe computers residing at the Martinsburg Computing Center.

In your report, you stated that the security-sensitive system components and settings for the Masterfile operating system were generally adequate but some improvements were needed. It is our management goal to continually strive for an enhanced security program that effectively manages risks. In that regard, we appreciate your comments that will further assist us in strengthening security documentation, systems software management, and logical access controls over the Masterfile system. See the attached detailed response to each of your report recommendations. Please note that Information Systems cited in your report has been changed to Information Technology Services, and this change is reflected in our response.

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

LIMITED OFFICIAL USE

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

**Management response to Draft Audit Report – Controls Over the Masterfile
System Are Generally Adequate, But Some Improvement Is Needed**

RECOMMENDATION #1

The Chief, Information Technology Services should ensure the security documentation for the Masterfile mainframe system is reviewed and made current and compete, according to existing Federal standards.

ASSESSMENT OF CAUSE:

The IBM Master File Mainframe received an unconditional Security Certification in 1996. A re-certification effort is now underway. The current certification process is manual and contributes to the process taking longer than desired. This fiscal year, with contractor assistance, we will be implementing an automated tool that will expedite the certification process.

CORRECTIVE ACTION TO RECOMMENDATION #1:

All security re-certification documentation is complete for the Masterfile mainframe system. The final step in the process is the completion of the Security, Test and Evaluation test plan.

IMPLEMENTATION DATE:

07/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Office of Cyber Security

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #2

The Chief, Information Technology Services should ensure that the Computer Security Plan for the Masterfile system includes specific requirements for periodic background investigations of individuals with sensitive system access of no less than every 5 years. These individuals should include, at a minimum, users with system-level attributes.

ASSESSMENT OF CAUSE:

MCC follows the IRS suggested format of the Computer Security Plan. A requirement for periodic background investigations of no less than every 5 years of individuals with sensitive system access is currently not included in the Computer Security Plan format.

CORRECTIVE ACTION TO RECOMMENDATION #2:

A management team composed of representatives from Martinsburg Computing Center, Office of Security Evaluation and Oversight, and Personnel Security will re-evaluate the Computer Security Plan and associated investigative requirements for sensitive system access.

IMPLEMENTATION DATE:

10/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Office of Security Evaluation and Oversight

Associate Director, Personnel Security

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

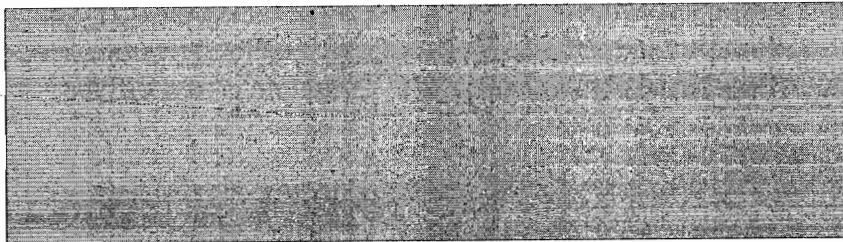
LIMITED OFFICIAL USE

RECOMMENDATION #3

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

A. Users with Multiple Group-Level Attributes:

ASSESSMENT OF CAUSE:



(b)(2),(b)(7)(E)

CORRECTIVE ACTION TO RECOMMENDATION #3:

Over the past several years, MCC has taken steps to considerably reduce the number of staff having this access. The unique nature of the work however periodically necessitates this access that deviates from the LEM. Whenever this occurs, the MCC Security and Disclosure Branch will prepare and submit a deviation request from the RACF LEM standard. The deviation request will include a justification for the deviation, including the steps to be taken to mitigate risks.

IMPLEMENTATION DATE:

10/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Security Evaluation and Oversight

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #3 (Continued)

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

B. Users with Multiple System-Level Attributes:

ASSESSMENT OF CAUSE:

Normally, only two Security Specialists are assigned both Resource Access Control Facility (RACF) System Special and System Auditor. During the review a third Security Specialist was assigned the System Auditor Attribute to his userid to fulfill investigative responsibilities and to provide information for the auditors. Periodically, a RACF Security Specialist will need to assign the System Auditor attribute to his/her userid for completion of tasks. However, as soon as the work is completed the attribute is removed.

CORRECTIVE ACTION TO RECOMMENDATION #3:

The System Auditor attribute was removed from the Security Specialist's userid after completion of the assigned tasks.

IMPLEMENTATION DATE:

Completed

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Security Evaluation and Oversight

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

LIMITED OFFICIAL USE

RECOMMENDATION #3 (Continued)

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

C. Users with Multiple UserIDs:

ASSESSMENT OF CAUSE:

Additional userids are assigned to Systems Programming Branch and Security and Disclosure Branch employees for testing purposes. These are low level userids used for testing and resolving normal level user problems and testing to insure Resource Access Control Facility (RACF) is providing its stated protection. An individual will be assigned more than one userid while they are on a detail. The first userid is placed in revoke status. When an individual is assigned to another work area the system will show that they have two userids for a 30-day period after they are assigned the new userid. This allows the user to copy or rename any data sets from the old userid to the new one. For this time period the user would be displayed as having two userids assigned.

CORRECTIVE ACTION TO RECOMMENDATION #3:

The unique nature of the work periodically necessitates deviating from the LEM. Whenever this occurs, the MCC Security and Disclosure Branch will prepare and submit a deviation request from the RACF LEM standard. The deviation request will include a justification for the deviation, including the steps to be taken to mitigate risks.

IMPLEMENTATION DATE:

10/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Security Evaluation and Oversight

5

LIMITED OFFICIAL USE

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #3 (Continued)

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

D. UserIDs Not Deleted After [REDACTED] of Inactivity:

(b)(2),(b)(7)(E)

ASSESSMENT OF CAUSE:

Intermittently, the MCC Security and Disclosure Branch performs a manual review of UserIDs that are inactive for [REDACTED] in order to delete them from the system.

(b)(2),(b)(7)(E)

CORRECTIVE ACTION TO RECOMMENDATION #3:

MCC Security and Disclosure Branch will schedule and monitor regular reviews of UserIDs that are inactive for [REDACTED] in order to delete them from the system. The reviews will support proper system maintenance and assist in ensuring the system complies with the LEM.

(b)(2),(b)(7)(E)

IMPLEMENTATION DATE:

7/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #3 (Continued)

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

(b)(2),(b)(7)(E)



ASSESSMENT OF CAUSE:

(b)(2),(b)(7)(E)



CORRECTIVE ACTION TO RECOMMENDATION #3:

(b)(2),(b)(7)(E)



performance problem arises as the result of this capability being activated, MCC Security and Disclosure Branch will prepare and submit a deviation request from the Resource Access Control Facility (RACF) LEM standard. The unique nature of the work does periodically necessitate deviating from the LEM. If a deviation request is needed, it will include a justification for the deviation, including the steps to be taken to mitigate risks.

IMPLEMENTATION DATE:

7/01/2001 to activate System-Level Auditing
10/01/2001 to request a deviation from the LEM (only if deemed necessary)

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Security Evaluation and Oversight

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #3 (Continued)

Director, MCC should correct the identified instances of non-compliance with the Law Enforcement Manual (LEM) on the Masterfile system or obtain approval to deviate from the LEM from the Office of Security Evaluation and Oversight (SEO).

F. Groups Assigned UserIDs with Incompatible Job Responsibilities:

ASSESSMENT OF CAUSE:

According to report findings, five users had incompatible job responsibilities. In a subsequent review of the UserIDs in which job functions differed from the defined duties for the group, we determined that the information provided to the auditors did not reflect the current status for those UserIDs. Individuals with the applicable UserIDs were either promoted to new job assignments or were on detail to another job. As a result, new UserIDs were being compared to the definition of the former job responsibilities.

CORRECTIVE ACTION TO RECOMMENDATION #3:

We reviewed applicable system definitions and determined that all data is now current.

IMPLEMENTATION DATE:

Completed

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #4:

The Director, MCC should obtain guidance from the Office of Security Evaluation and Oversight (SEO) on the issue of [REDACTED] deviation request from the Law Enforcement Manual (LEM) for the requirement to the SEO.

(b)(2),(b)(7)(E)

ASSESSMENT OF CAUSE:

[REDACTED]

(b)(2),(b)(7)(E)

CORRECTIVE ACTION TO RECOMMENDATION #4:

MCC Security and Disclosure Branch will prepare and submit a deviation request from the Resource Access Control Facility (RACF) LEM standard. The request will include a justification for the deviation, including the steps to be taken to mitigate risks.

IMPLEMENTATION DATE:

10/01/2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Director, Office of Security Evaluation and Oversight

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #5 (b)(2),(b)(7)(E)

The Chief, Information Technology Services should ensure that reviews of the Masterfile system are performed [REDACTED] to ensure that its access controls are in compliance with the IRS' Resource Access Control Facility (RACF) Law Enforcement Manual (LEM).

ASSESSMENT OF CAUSE:

Due to the exigency of work assignments given to the Office of Security Evaluation and Oversight (SEO) and activities required by Presidential Decision Direction PDD-63 for Critical Infrastructure Protection, several onsite reviews, including the review of the Martinsburg Computing Center, were suspended during FY 2000. Prior to that, the computing center and Masterfile were [REDACTED] During FY 1999, the computing center received both an oversight review visit and a problem resolution visit.

(b)(2),(b)(7)(E)

CORRECTIVE ACTION TO RECOMMENDATION #5:

An onsite review of the Martinsburg Computing Center and the Masterfile system was performed by SEO the week of April 23 through April 27, 2001. In addition, SEO analysts are gaining remote access to Masterfile to conduct periodic, unannounced online reviews of the Masterfile system to ensure that its access controls are in compliance with the RACF LEM and other requirements. These [REDACTED]

(b)(2),(b)(7)(E)

IMPLEMENTATION DATE:

Closed, onsite review conducted week of April 23, 2001
Periodic online reviews will begin May, 2001

RESPONSIBLE OFFICIAL:

Director, Office of Security Evaluation and Oversight

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

LIMITED OFFICIAL USE

RECOMMENDATION #6:

The Director, MCC should ensure that the Authorized Program Facility (APF) libraries are closely monitored, including devising a control mechanism to alert systems programmers at initial program load (IPL) of APF authorized libraries that are not on volumes specified in the APF list.

ASSESSMENT OF CAUSE:

After a product was removed, the APF inadvertently retrieved an entry for that product.

CORRECTIVE ACTION TO RECOMMENDATION #6:

MCC will write a utility program that will read the Progxx members of Parmlib and report any discrepancies. This will be a ControlM job that will execute at least once a week. Notification of any discrepancies will be sent to various systems programmers and managers.

IMPLEMENTATION DATE:

August 31, 2001

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

LIMITED OFFICIAL USE

RECOMMENDATION #7:

The Director, MCC should develop procedures for periodically reviewing the contents of APF libraries to ensure that instances of duplicate programs are reduced.

ASSESSMENT OF CAUSE:

MCC has numerous products from the same vendor but are at different maintenance levels. Thus, there always will be some duplication of modules in the APF libraries.

CORRECTIVE ACTION TO RECOMMENDATION #7:

MCC implemented procedures for a system monitoring program to periodically produce a report of the duplicate modules. This report is being reviewed to ensure there are no unnecessary duplication of modules.

IMPLEMENTATION DATE:

Completed

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

12

LIMITED OFFICIAL USE

**Controls Over the Masterfile System Are Generally Adequate,
But Some Improvement Is Needed**

LIMITED OFFICIAL USE

RECOMMENDATION #8:

The Director, MCC should ensure that system password formats are removed from the MCC Intranet.

ASSESSMENT OF CAUSE:

Password formats were placed on the intranet to electronically provide users with the security procedures and to reinforce security awareness.

CORRECTIVE ACTION TO RECOMMENDATION #8:

System password formats were removed from the Intranet.

IMPLEMENTATION DATE

Completed

RESPONSIBLE OFFICIAL:

Director, Martinsburg Computing Center

Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed

LIMITED OFFICIAL USE

RECOMMENDATION #9:

The Director, MCC should restructure the password formats for the Masterfile system to increase the complexity of the passwords, thus making them more difficult to guess or crack.

ASSESSMENT OF CAUSE:

The passwords are in compliance with all IRS and Federal Government requirements. In addition, the system revokes a userid (rendering it unusable until resumed by a system security administrator) after three unsuccessful password attempts. These factors mitigate the risk of being compromised by a hacker. As long as users follow the standards when creating passwords (and this applies to all systems regardless of password format) the risk is greatly reduced.

CORRECTIVE ACTION TO RECOMMENDATION #9:

A management team led by the Office of Security Evaluation and Oversight, and assisted by MCC, will assess the adequacy of existing passwords and conduct a feasibility study for restructuring password formats.

IMPLEMENTATION DATE:

Feasibility study to be completed 10/31/2001

RESPONSIBLE OFFICIAL:

Director, Office of Security Evaluation and Oversight

Director, Martinsburg Computing Center