The Internal Revenue Service Can Increase Storage Capacity on Several IBM Mainframe Systems Through Improved Maintenance

November 1999

Reference Number: 2000-20-009

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 12, 1999

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Can Increase Storage Capacity on Several IBM Mainframe Systems Through Improved Maintenance

This report presents the results of our review of selected general controls of the Multiple Virtual Storage (MVS) operating system on two of the Internal Revenue Service's (IRS) mainframe computers. The two systems we reviewed were the Masterfile system, which serves as the platform for the primary processing of all taxpayer accounts, and the Automated Collection/Integrated Collection Program Development System, which is used to develop and test the IRS' computer systems for collecting delinquent taxes.

In summary, we found that the general controls over the IBM systems included in our review were adequate to provide system security and safeguard sensitive data; however, system storage capacity could be increased if extraneous files were removed from the system. We recommended that IRS management develop procedures to periodically examine system storage space to identify extraneous data files and programs, and to ensure they are removed from the systems.

Management agreed with our recommendation and has taken corrective action. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

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

Table of Contents

Executive Summary

The Internal Revenue Service (IRS) uses IBM's Multiple Virtual Storage (MVS) operating system for many of its mission critical, tax processing systems. We examined the controls on two of these systems: the Masterfile system, which serves as the platform for the primary processing of all taxpayer accounts, and the Automated Collection System/Integrated Collection program development system (ACS/ICS), which is used to develop and test the IRS' computer system for collecting delinquent taxes. Because the MVS operating system is used on IRS computers that maintain over 206 million taxpayer accounts, its implementation must be closely controlled and monitored.

The objective of this review was to determine if selected general controls of the MVS operating system were implemented to provide system security, safeguard sensitive data, and ensure efficient use of system resources.

Results

Generally, the controls of the two MVS operating systems we reviewed were adequate to provide system security and to safeguard sensitive data. We determined, however, that system resources could be better used if extraneous files were removed from the systems.

System Controls Were Adequate to Provide System Security and Protect Sensitive Data

System resources were adequately protected and controls over program files and libraries containing operating system files assured that only authorized personnel had access to these significant system resources. In addition, the MVS operating system was implemented in a manner that provided IRS with necessary management information. Specifically, we found:

- Key System Management Facility (SMF)[1] settings were properly implemented on both systems.
- Exits (automated system interfaces) that can be used to suppress selected audit trail data were not in use.

[1] SMF is an IBM product that serves as an event tracking mechanism and audit trail for system activities in MVS.

- "ZAP" programs[2] were adequately protected, and access to these programs was restricted on both systems.
- Systems security controls were employed to protect key system resources such as the Authorized Program Facility (APF) and the Time-Sharing Option (TSO) User Attribute Set.[3]

In some instances, IRS systems programmers took immediate action and made changes on-line based on our verbal recommendations for improving system control settings.

Storage Capacity Can Be Increased by Removing Unnecessary Files

Our review of the Masterfile and ACS/ICS systems identified a significant number of files that were uncataloged (not maintained or recognized by the MVS facility for organizing files) or miscataloged (contained in one disk unit and "labeled" as being in another). On the taxpayer account processing system, we found that over 8 percent of the over 10,600 files on the disk units containing important system set-up files were uncataloged or miscataloged. On the development system, 25 percent of the over 37,000 files on the system were uncataloged or miscataloged. Allowing extraneous files to remain on the system wastes valuable storage space. Furthermore, extraneous files present a system security risk since they may be altered to support unauthorized activities.

Summary of Recommendation

The Chief Information Officer should develop procedures to periodically examine system storage space to identify extraneous data files and programs, and to ensure that they are removed from the systems.

Management's Response: IRS management has implemented the Hierarchical Storage Manager, which ages off and archives data files that have not been used. Also, batch jobs

[2] ZAP programs can be used to alter or delete the Volume Table of Content (VTOC), which is the "card catalog" for the entire system. Without a reliable VTOC, files cannot be found in the system.

[3] APF programs can circumvent all standard MVS security mechanisms and gain access to secured data. The TSO User Attribute Set houses the powers granted to each user on the system.

that eliminate uncataloged data files have been instituted as part of weekly housekeeping batch runs.

Objective and Scope

We reviewed the IRS' Masterfile system and ACS/ICS development system.

This report presents the results of our review of selected general controls of the Multiple Virtual Storage (MVS) operating system on two of the Internal Revenue Service's (IRS) mainframe computers. The two systems we reviewed were the Masterfile system, which performs the primary processing of all taxpayer accounts, and the Automated Collection/Integrated Collection program development system (ACS/ICS), which is used to develop and test the IRS' computer systems for collecting delinquent taxes. The objective of this review was to determine if selected general controls of the MVS operating system were implemented to provide system security, safeguard sensitive data, and ensure efficient use of system resources. Fieldwork was initiated in June 1998 and completed in May 1999. The extended audit period was due to reprioritization of audit assignments after audit staff turnover.

We selected the MVS operating system for review because it is widely used throughout the IRS on systems that contain sensitive data and has a material influence on system processing. To facilitate our review of the operating system, we used Computer Associates' CA-Examine[1] audit tool. The CA-Examine tool analyzes data in the operating system and produces information to identify both system control weaknesses and computer resource management concerns. Specifically, the CA-Examine tool generated valuable information on how security controls and resource management could be improved within the MVS operating system.

[1] CA-Examine is an on-line interactive software package that performs an analysis of the hardware and software environment of a MVS system. It provides information about system security, integrity, and control mechanisms that is difficult to obtain from other sources.

We conducted this review within the office of the Chief Information Officer. The scope of our review included testing on the computers located at the Martinsburg Computing Center (MCC). On-site interviews were conducted with system administrators and Resource Access Control Facility (RACF) personnel in the National Office for the ACS/ICS development system and at MCC for the Masterfile system. This review was conducted 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.

Background

The IRS uses the MVS operating system to perform a significant part of its mission critical tax processing.

The IRS uses IBM's MVS operating system on its IBM and IBM compatible mainframe computers. These computers perform a significant part of the IRS' mission critical tax processing, including the maintenance of information for over 206 million taxpayer accounts. The MVS operating system schedules program processing, controls subsystem use, and monitors system activity. It can also process user commands that direct control of certain file and program processing activities and that determine where the resulting output will be placed on the system. In addition, the System Management Facility (SMF) is set up and controlled within the MVS operating system. SMF parameters establish the audit trail, which capture accesses at the operating system level, and can be set up to gather varying amounts of data about the utilization of system resources.

Results

At the time of our review, the controls over the two IBM compatible systems were adequate to protect system

resources and sensitive data. However, we also determined that system resources could be better used if extraneous files were removed from the systems.

System Controls Were Adequate to Provide System Security and Protect Sensitive Data

Computer environments require continual monitoring of operating system settings and parameters.

The MVS operating system controls over the Masterfile system and the ACS/ICS program development system were adequate to provide system security and to safeguard sensitive data residing on those systems. Systems settings and parameters, as well as the protection of user-ids (the identifier used by an individual to log onto a system) and files can change rapidly in any computer environment. The controls we reviewed will remain effective as long as the IRS continues to monitor its operating system environment.

Controls over the system libraries and program files were adequate to assure that only authorized personnel had access to these important system resources. In addition, we determined that the MVS operating system was capturing the necessary system management information to monitor significant activities on the system.

Specifically, we found:

- Key System Management Facility (SMF) settings were properly implemented on both systems.
- Exits (automated system interfaces) that can be used to suppress selected audit trail data were not in use.
- "ZAP" programs were adequately protected, and access to these programs was restricted on both systems. ZAP programs can be used to alter or delete the Volume Table of Contents (VTOC) which is the "card catalog" for the entire system. Without a reliable VTOC, files cannot be found in

the system.

- Systems security controls were employed to protect key system resources such as the Authorized Program Facility (APF) and the Time-Sharing Option (TSO) User Attribute Set. Protection of these resources is important. APF programs can circumvent all standard MVS security mechanisms and gain access to secured data. The TSO User Attribute Set houses the powers granted to each user on the system.

In some cases, IRS systems programmers made changes on-line based on changes to system settings we recommended in discussions. These instances and our assessment of system resource protections are presented in more technical detail in Appendix IV.

Storage Capacity Can Be Increased by Removing Unnecessary Files

Valuable storage space was lost due to a significant number of data files that were not maintained or recognized by the MVS file structure.

Significant numbers of data files, 8 percent on one system and 25 percent on the other, were uncataloged (not maintained or recognized by the MVS facility for organizing files) or miscataloged (contained in one disk unit and "labeled" as being in another). According to the CA-Examine MVS Usage Guide, uncataloged files waste valuable storage space. Furthermore, extraneous files present a system security risk as they may be altered to support unauthorized activities.

The Masterfile system contains over 1,400 disk storage units (volumes). Due to the extensive amount of data produced by the CA-Examine volume scan function, we prioritized the volumes on which to run the scan. We selected the volumes that contain critical system setup files and authorized programs (SYS volumes). Over 8 percent of the 10,693 files on the SYS volumes were uncataloged (570 files) or miscataloged (325 files).

A volume scan of the 11 volumes containing files used for initializing the system (RES volumes) and a sample of 17 production volumes returned relatively low numbers of uncataloged files (22 files), most of which were VTOC index files.

Due to the smaller size of the ACS/ICS development system, we ran the volume scan on all of the system's volumes. Twenty-five percent of the 37,574 files on the system were either uncataloged (8,621 files) or miscataloged (636 files).

IBM-supplied utility programs provide many useful functions, such as copying and listing data files and maintaining source libraries. Uncataloged or miscataloged data files can result when system programmers use IBM-supplied utilities for copying or moving data files, and they do not code parameters that remove the original file from the catalog or rename the copied file. In addition, we found that no formal procedures exist for the removal of uncataloged and miscataloged files.

Recommendation

1. The Chief Information Officer should develop procedures to periodically examine system storage space to identify extraneous programs and data files, and to ensure that they are removed from the system.

Management's Response: Management has implemented the Hierarchical Storage Manager, which ages off and archives data files that have not been used. In addition, batch jobs that eliminate uncataloged data files have been added to weekly housekeeping batch runs.

Conclusion

The MVS operating system controls over the Masterfile system and the ACS/ICS program development system were adequate to provide system security and to safeguard sensitive data residing on those systems. Systems settings and parameters, as well as the protection of user-ids and files, can change rapidly in any computer environment. The controls we reviewed will remain effective as long as the IRS continues to monitor its operating system environment.

Controls over the system libraries and program files were adequate to assure that only authorized personnel had access to these important system resources. In addition, we determined that the MVS operating system was capturing the necessary system management information to monitor significant activities on the system. However, we also determined that system resources could be better used if extraneous files were removed from the systems.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to determine if selected general controls of the Multiple Virtual Storage (MVS) operating system were implemented to provide system security, safeguard sensitive data, and ensure efficient use of system resources. We reviewed two IBM compatible Internal Revenue Service (IRS) mainframe systems: the Masterfile system, which is the platform for the primary processing of all taxpayer accounts, and the Automated Collection/Integrated Collection program development system, which is used to develop and test IRS' computer systems for collecting delinquent taxes.

To facilitate our review of the MVS operating system, we used Computer Associates' CA-Examine audit tool. The IBM MVS operating system was selected for review because it is widely used throughout the IRS on systems that contain sensitive data. Analysis of the information produced from the CA-Examine tool can identify improvements needed to address both system control weaknesses and computer resource management concerns. Specifically, the CA-Examine tool generates valuable information on how security controls and resource management could be improved within the MVS operating system.

In addition, the results of this review will be used to establish benchmark system parameters against which subsequent MVS reviews of these systems will be measured. Future reviews will entail periodic installation of the CA-Examine audit software on the mainframes to take a "snapshot" of system parameters. The snapshot will be measured against the baseline we established in this review.

The scope of this review encompassed the review of the adequacy of audit trail settings to monitor computer activities; the protection of MVS libraries, programs and files; the effectiveness of system configuration; and the efficient use of system resources. Specifically, we:

I. Reviewed system management information to determine if system settings provided an adequate audit trail to monitor computer activities.

   A. Obtained background information to gain a general understanding of the computer operating environment.

   B. Reviewed the Systems Management Facility parameters, the primary audit trail in the MVS environment, to ensure that an adequate audit trail was established, and system security was properly maintained.

II. Reviewed the MVS library, program, and file authorization parameters established to determine if system resources were adequately protected.

A. Reviewed the MVS library, program, and file authorization parameters to determine whether they adequately protected system resources.

B. Reviewed the Authorized Program Facility to ensure access restrictions adequately protected system resources.

C. Reviewed the Time-Sharing Option User Attribute Set (SYS1.UADS) to ensure that user information, including passwords, was not accessible to other system users.

D. Identified sensitive files and ensured that the Resource Access Control Facility provided adequate security of this data.

III. Reviewed the MVS system configuration and related components including appendages, system exits, system libraries, the Program Properties Table, and supervisor calls to identify possible security exposures.

A. Reviewed system appendages controlling input/output processing and ensured that their modification or use was properly authorized.

B. Reviewed system exits to ensure that they were only used to perform appropriate system functions.

C. Reviewed the Link Pack Area (LPA) to determine if LPA libraries were adequately protected, and their modules configured, to support efficient systems operations.

D. Reviewed the Program Properties Table to identify those programs having special MVS capabilities. Also, ensured that these capabilities were not excessive and access to these programs was adequately restricted.

E. Reviewed supervisor calls to ensure that they could not be used to improperly alter system data.

IV. Determined if system storage space was efficiently used. Identified uncataloged and miscataloged files and determined if they could be removed from the system.

Appendix II

Major Contributors to This Report

Scott Wilson, Associate Inspector General for Audit (Information Systems Programs)
Mike Phillips, Acting Director, Office of Audit Projects
Kent Sagara, Acting Deputy Director, Office of Audit Projects
Vincent Dell'Orto, Audit Manager
Anthony Knox, Senior Auditor
Gwen Bryant-Hill, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Deputy Chief Information Officer, Systems IS
Deputy Chief Information Officer, Operations IS
Assistant Commissioner (Program Evaluation and Risk Analysis) M:OP
Director, Systems Support Division IS:S:SS
Director, Martinsburg Computing Center IS:O:M
National Director for Legislative Affairs CL:LA
Office of the Chief Counsel CC
Office of Management Controls M:CFO:A:M
Audit Liaison (Attn: Barry Herrmann) IS:I:IS:O:A

Appendix IV

Details of Systems Resource Protections

System resources were adequately protected through the Multiple Virtual Storage (MVS) operating system, program, and file authorization parameters. In addition, we determined that the MVS operating system was capturing necessary system management information.

Specifically, we found:

- The key System Management Facility (SMF) settings, which control the primary audit trail in the MVS environment, were enabled on both systems. SMF collects information about MVS events such as Time-Sharing Option (TSO) logons, logoffs, job starts and ends, and file access. On the Masterfile system, we found that the system's Initial Program Load (IPL) record, which automatically records when the system is reset or initialized, was not turned on. Systems software personnel agreed to change the system's IPL record and allow on-line logging of system initiation instead of manual logging, as is currently employed. For the Automated Collection System/Integrated Collection System (ACS/ICS) development system, all key SMF records were active.

- Exits IEFU83, IEFU84, and IEFU85, which can be used to cancel SMF records, were not active on either system. These exits are expressly provided to suppress SMF exits. On the Masterfile system, our initial CA-Examine query showed that IEFU83 and IEFU84 were active. However, after discussions with systems software personnel, we reviewed the EXITS parameter in the SMFPRM00 member of IEASYS00. The exits were not specified in this member, and according to IBM documentation, are not active. The CA-Examine query for the ACS/ICS development system showed no exits were active.

- "ZAP" programs, which can alter or zap the Volume Table of Contents (VTOC), were adequately protected, and access to these programs was restricted on both systems. On the Masterfile system, we located the AMASPZAP and IMASPZAP programs in SYS1.SECURLIB. We verified that SYS1.SECURLIB had restricted access. According to the Resource Access Control Facility (RACF) profile for this datasheet, only one user has ALTER access. No ZAP programs were found on the ACS/ICS development system.

- RACF controls were employed to protect key system resources such as the Authorized Program Facility (APF) and the TSO User Attribute Set (SYS1.UADS). It is important to protect the APF because APF authorized programs can circumvent all standard MVS security mechanisms and gain access to secured data. SYS1.UADS must be protected because the user attribute file resides there. This

file defines the powers granted to each user on the system. SYS1.UADS is not automatically password-protected, nor is the information encrypted. Anyone with proper access authority can read and modify SYS1.UADS.

With a SETROPTS RACF report, we determined RACF was active and the PROTECTALL option was employed. We were unable to access APF authorized libraries or SYS1.UADS. We subsequently requested a RACF file profile for each system. Both were adequate to protect from unauthorized accesses. In addition, the default IBMUSER user-id, which has unlimited powers, was revoked on both systems.

Appendix V

Glossary of Terms

Authorized Program Facility (APF) – the key security feature of the operating system under the user's control. Programs that meet APF-authorization requirements can issue a supervisor call to switch themselves into "supervisor state." Programs in "supervisor state" are permitted to execute privileged machine instructions. APF-authorized programs can circumvent or disable all security mechanisms, including access control software, and access all production data. Customer data centers are responsible for maintaining the contents and integrity of the APF library system.

Exits – user-written programs that obtain control at decision-making points in the vendor's software. Exits are usually written in Assembler language by a systems programmer.

IBM Compatible – mainframes developed and marketed by IBM, or mainframes produced by other companies that mimic the IBM mainframes and run the MVS operating system.

Multiple Virtual Storage (MVS) – the operating system on the IBM mainframes. The MVS operating system manages hardware, programs and data; schedules and runs work; balances system resources; and allocates resources.

Resource Access Control Facility (RACF) – an access control security package for IBM's MVS operating system and Virtual Machine environment. It provides data security protection by identifying and verifying users entering the system, restricting access to protected resources to authorized resources, restricting capabilities of authorized users once they gain access to protected resources, and logging and reporting security-related events.

System Management Facility (SMF) – collects information about MVS system events and produces an audit trail of MVS system events by recording events in SMF files. SMF writes records for events such as: logon/logoff of TSO users, reconfiguration of devices, initiation and termination of jobs, signon and signoff of NJE users, and system status information.

Time-Sharing Option (TSO) User Attribute File (UADS) – list of users authorized to use TSO. UADS is a partitioned file. Each member of UADS identifies an individual TSO user and includes the user's identity, password, account number, and logon procedure. This dataset is usually called SYS1.UADS and is important because it defines the powers granted to each TSO user on the system.

Volume Table of Contents (VTOC) – a sequential file that is on every volume. The

records of the VTOC contain physical pointers (addresses) to the file, the file name, the file size, and the file record length.

Appendix VI

Management's Response to the Draft Report

COMMISSIONER

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

October 5, 1999

OFFICE OF TREASURY
INSPECTOR GENERAL
RECEIVED
199910-4CF-JN MDH
1999 OCT -7 A 10:12
FOR TAX ADMINISTRATION

MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Management Response to Draft Audit Report – The Internal Revenue Service Can Increase Storage Capacity on Several IBM Mainframe Systems Through Improved Maintenance

Thank you for giving me the opportunity to review and comment on your draft report and recommendation on our ability to increase storage capacity on IBM mainframe systems through improved maintenance.

We have implemented automated storage management systems, which improve maintenance on our mainframe systems. The attached management response provides more information on the capabilities of these storage management systems.

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

Attachment

cc: Associate Inspector General for Audit (Information Systems Programs)

RECOMMENDATION

The Chief Information Officer should develop procedures to periodically examine system storage space to identify extraneous programs and data files, and to ensure that they are removed from the system.

ASSESSMENT OF CAUSE

At the time of this review, the controls over the two IBM compatible systems were adequate to protect system resources and sensitive data. However, it was determined that system resources could be better used if extraneous files were removed from the systems.

CORRECTIVE ACTION

All security reviews of our system have verified that we are not running with RACF (security) exits and have never seen a need or requirement to suppress audit trail data. We use System Managed Facility (SMF) for records in the 80's series for DSMON and RACF Report Writer reports both here and in the field.

As to efficient use of system resources, we have implemented the Hierarchical Storage Manager (HSM) which ages off and archives datasets which have not been used. The SMF, which controls the allocation of datasets (and always catalogues them), assures that it is highly unlikely that we have large numbers of unused or uncataloged datasets on our system. As a part of our weekly housekeeping batch runs, we run a job that scratches uncataloged datasets.

IMPLEMENTATION DATE

COMPLETED: August 16, 1999 **PROPOSED: __N/A__**

RESPONSIBLE OFFICIAL

Chief Information Officer IS
Deputy Chief Information Officer (Systems) IS
Assistant Commissioner for Systems Development IS:S

CORRECTIVE ACTION MONITORING PLAN

With the implementation of HSM and SMF, as well as the removal of an obsolete system, no further action is required at this time.