

**Management Advisory Report: The  
Configuration of a Security and  
Communications System Backup Computer  
Environment Is Not Compliant With  
Internal Revenue Service Requirements**

**June 2002**

**Reference Number: 2002-20-109**

**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 28, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &  
CHIEF INFORMATION OFFICER

*Scott E. Wilson*

FROM: (for) Pamela J. Gardiner  
Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report - The Configuration of a  
Security and Communications System Backup Computer  
Environment Is Not Compliant With Internal Revenue Service  
Requirements (Audit # 200220043)

This report presents the results of our review of the configuration of a Security and Communications System (SACS) backup computer environment at the Tennessee Computing Center (TCC). The overall objective of this review was to evaluate the configuration management and security controls over the SACS non-production mainframe computer at the TCC. Issues relating to this computer were identified from our review of the Internal Revenue Service's (IRS) SACS mainframe production processing environment.<sup>1</sup>

The SACS mainframe environment is a critical component of the IRS' customer service efforts, providing front-end access and security services to two mission critical systems: the Integrated Data Retrieval System (IDRS) and the Corporate Files On-Line System. Through these systems, designated IRS employees have online access to certain taxpayer information.

In summary, we found that the configuration of the non-production, or backup, SACS mainframe computer environment at the TCC is not compliant with IRS requirements. Specifically, the audit trail reporting capabilities for this computer have not been enabled. This condition occurred because changes to the configuration of this backup mainframe, as part of a disaster recovery conversion, were not approved by the required configuration control board. As a result, further changes to the backup mainframe configuration, which included the implementation of audit trail reporting

---

<sup>1</sup> *The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made* (Reference Number 2002-20-044, dated January 2002).

capabilities, were halted. Without these capabilities, any user actions originating on this backup mainframe computer would not be reported to management. Such actions may include unmonitored access to sensitive Martinsburg Computing Center (MCC) IDRS employee and network configuration information.

We recommended that the Chief, Information Technology Services (ITS), ensure that the SACS backup mainframe computer at the TCC is restored to an approved configuration, including the removal of all sensitive MCC IDRS employee and network configuration information. In addition, the Chief, ITS, should ensure that future software and other configuration changes to the SACS backup mainframe computer at the TCC follow the Systems Support Division configuration management process.

Management's Response: IRS management agreed with the recommendations presented in the report. Corrective actions will be taken to restore the SACS backup mainframe computer to an approved configuration and ensure that future software and other configuration changes to this computer follow the approved configuration management process. Management's complete response to the draft report is included as Appendix IV.

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

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

**Table of Contents**

Background ..... Page 1

Configuration of a Security and Communications System Backup  
Mainframe Environment Is Not Compliant With Internal Revenue  
Service Requirements ..... Page 1

Recommendation 1: ..... Page 3

Recommendation 2: ..... Page 4

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 5

Appendix II – Major Contributors to This Report..... Page 6

Appendix III – Report Distribution List ..... Page 7

Appendix IV – Management’s Response to the Draft Report ..... Page 8

## **Management Advisory Report: The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements**

---

### **Background**

---

The Security and Communications System (SACS) is a critical component of the Internal Revenue Service's (IRS) customer service efforts, providing front-end access and security services to two mission critical systems: the Integrated Data Retrieval System (IDRS) and the Corporate Files On-Line System. Through these systems, designated IRS employees have online access to certain taxpayer information. The SACS environment processes transactions and data through the SACS mainframe computers and the ICS/ACS/PRINT<sup>1</sup> (IAP) mainframe computers, both located at the Tennessee (TCC) and Martinsburg Computing Centers (MCC).

Issues relating to this computer were identified during our review of the IRS' SACS mainframe production processing environment.<sup>2</sup> Audit work was performed on-site at the TCC and at the National Headquarters in the Office of the Chief, Information Technology Services, during October 2001. The scope of our review was limited to this non-production mainframe because the prior review focused on the SACS production environment. This review was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The configuration of the non-production, or backup, SACS mainframe computer environment at the TCC is not compliant with IRS requirements. Specifically, the audit trail reporting capabilities for this computer have not been enabled. This occurred because changes to the configuration of this backup mainframe, as part of a disaster recovery conversion, were not approved by the required

---

### **Configuration of a Security and Communications System Backup Mainframe Environment Is Not Compliant With Internal Revenue Service Requirements**

---

---

<sup>1</sup> Integrated Collection System (ICS)/Automated Collection System (ACS)/Printer Replacement to Integrate New Tools (PRINT).

<sup>2</sup> *The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made* (Reference Number 2002-20-044, dated January 2002).

## **Management Advisory Report: The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements**

---

configuration control board. As a result, further changes to the backup mainframe configuration, which included the implementation of audit trail reporting capabilities, were halted. Without these reporting capabilities, any user actions originating on this mainframe computer would not be reported to management. Such actions could include unmonitored access to sensitive employee and network configuration information.

IRS policies require the creation of user activity reports, from system audit trails, and their distribution to appropriate managers for review for all IRS information systems. In addition, IRS policies require that a configuration management process must be implemented for all IRS information systems. The IRS' Systems Support Division (SSD) has implemented a configuration management process to control software and configuration changes to many of the IRS' systems, including the SACS mainframe computers. This process, which is outlined in the SSD configuration management plan, includes the approval of all system changes by the SSD configuration control board.

The backup SACS mainframe environment is currently not configured to produce audit trail reports of user activity for management review. Specifically, the support environment needed to generate reports of IDRS user activity, from the IDRS application audit trail, has not been enabled. This environment would reside on the IAP mainframe located at the TCC. In addition, the support console for this computer has not been configured to enable the review of user activity at the system-level through the system audit trail.

This situation occurred because an initiative to convert the non-production SACS mainframe computer at the TCC to a backup system for the MCC SACS production mainframe environment was halted before audit trail reporting capabilities could be enabled. This conversion was one of two options specified in the October 2000 SACS disaster recovery plan and the one that the TCC chose to implement. In November 2000, as the TCC was preparing to test the telecommunications connectivity for its backup mainframe computer, the SSD halted the test since the SSD

## **Management Advisory Report: The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements**

---

configuration control board had not approved the conversion of this computer.

Since that time, further changes to the configuration of this backup computer at the TCC, including the implementation of audit trail reporting capabilities, have been delayed pending a decision on the long-term disaster recovery approach for the SACS mainframe environment. Currently, the SACS backup mainframe computer at the TCC serves as a backup processor for the TCC SACS production mainframe computer. Since this computer has been idle since November 2000, the operating system and data residing on it are out-of-date. Consequently, future use of the backup mainframe computer, other than as a backup processor for the TCC SACS production mainframe, would require a complete shutdown and reload of the current version of the operating system and any necessary data.

While the SACS backup mainframe at TCC is not a production system, sensitive information is nonetheless stored on it. In particular, sensitive MCC IDRS employee information as well as network configuration information is stored on the computer. Consequently, precautions must be taken to safeguard this sensitive information while the backup computer is in its current state, given that the audit trail monitoring and reporting capabilities have not been implemented.

### **Recommendations**

The Chief, Information Technology Services, should:

1. Ensure that the SACS backup mainframe computer at the TCC is restored to an approved configuration, including the removal of all sensitive MCC IDRS employee and network configuration information.

Management's Response: The Director, Enterprise Operations, will ensure that the SACS backup mainframe computer at the TCC is restored to an approved configuration, including the removal of all sensitive MCC IDRS employee and network configuration information.

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

This action will be verified by the SSD and TCC during SACS disaster recovery testing.

2. Ensure that future software and other configuration changes to the SACS backup mainframe computer at the TCC follow the SSD configuration management process.

Management's Response: The Director, Enterprise Operations, will ensure that future software and other configuration changes to the SACS backup mainframe computer at the TCC follow the SSD configuration management process. This action will be accomplished through regularly scheduled conference calls among the SSD, TCC, and MCC, where SACS configuration changes will be reviewed and discussed.



**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

**Appendix I**

**Detailed Objective, Scope, and Methodology**

The overall objective of this review was to evaluate the configuration management and security controls over the Security and Communications System (SACS) non-production, or backup, mainframe computer at the Tennessee Computing Center (TCC).

- I. Determined whether the TCC backup mainframe computer is following the configuration management process for the SACS environment.
  - A. Identified changes implemented on the TCC backup mainframe computer.
  - B. Determined whether any changes made to the TCC backup mainframe computer were submitted and approved through the Systems Support Division configuration management process.
- II. Determined whether sufficient access controls are in place on the TCC backup mainframe computer.
  - A. Determined whether user activity audit reports, generated from the system audit trail, are produced and forwarded to the appropriate managers for review.
  - B. Determined whether the SACS console support computers are properly configured to record system events.

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

**Appendix II**

**Major Contributors to This Report**

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)

Gary Hinkle, Director

Michael Howard, Acting Audit Manager

Myron Gulley, Senior Auditor

Steven Gibson, Auditor

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

**Appendix III**

**Report Distribution List**

Commissioner N:C  
Deputy Commissioner N:DC  
Chief, Information Technology Services M:I  
Director, Office of Security Services M:S  
Director, Enterprise Computing Centers M:I:E  
Director, Enterprise Operations M:I:E  
Director, Enterprise Technical Support Services M:I:E  
Director, Martinsburg Computing Center M:I:E:MC  
Director, Systems Support Division M:I:E:SS  
Director, Tennessee Computing Center M:I:E:TC  
Manager, Program Oversight and Coordination M:SP:P:O  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O  
Office of Management Controls N:CFO:F:M  
Audit Liaisons: Enterprise Operations M:I:E  
                  Office of Security Services M:S  
                  Program Oversight and Coordination M:SP:P:O

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

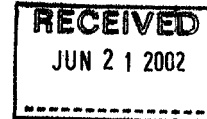
Appendix IV

**Management's Response to the Draft Report**



DEPUTY COMMISSIONER


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



June 20, 2002

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX  
ADMINISTRATION

FROM:

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

SUBJECT:

Management Response to the Draft Management Advisory  
Report – "The Configuration of a Security and Communications  
System Backup Computer Environment Is Not Compliant With  
Internal Revenue Service Requirements" (#200220043)

The Modernization, Information Technology & Security Services organization is committed to ensuring the security of sensitive taxpayer information. The Security and Communication System (SACS) mainframe provides front-end security access to the Integrated Data Retrieval System and the Corporate Files On-Line Systems that contain taxpayer information.

SACS monitors all IRS employee transactions with taxpayer databases to ensure that employee actions are appropriate. As such, SACS is a critical component of IRS' customer service efforts.

We maintain the SACS production mainframe in an approved configuration, using the Systems Support Division configuration management process for software and other configuration changes. As recommended in your report, we have taken action to:

- Restore the SACS non-production (backup) mainframe computer at Tennessee Computing Center (TCC) to an approved configuration, including removal of sensitive Martinsburg Computing Center (MCC) IDRS employee and network configuration information
- Follow the Systems Support Division configuration management process for future software and other configuration changes to the SACS backup mainframe computer

I have included additional details in my attached management response. If you have any questions, please call me at (202) 622-6800. Your staff can call Thomas Mulcahy, Manager, Program Oversight and Coordination Office, at (202) 283-6063.

Attachment

**Management Advisory Report: The Configuration of a  
Security and Communications System Backup Computer Environment  
Is Not Compliant With Internal Revenue Service Requirements**

---

**Attachment**

**Management Response to Draft Management Advisory Report – “The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements” (#200220043)**

**Recommendation #1**

The Chief, Information Technology Services, should ensure that the SACS backup mainframe computer at the TCC is restored to an approved configuration, including the removal of all sensitive MCC IDRS employee and network configuration information.

**Assessment of Cause**

The configuration of the non-production Security and Communication System (SACS) mainframe computer environment at the Tennessee Computing Center (TCC) is not compliant with IRS requirements, since the audit trail reporting capabilities were not enabled. The required configuration control board did not approve changes to the configuration of this backup mainframe as part of a disaster recovery conversion. As a result, we stopped further changes to the backup mainframe configuration, including implementation of audit trail reporting capabilities. Without these capabilities, any user actions originating on this backup mainframe computer would not be reported to management.

**Corrective Action #1**

The Director, Enterprise Operations will ensure that the SACS backup mainframe computer at the TCC is restored to an approved configuration and remove all sensitive Martinsburg Computing Center (MCC) Integrated Data Retrieval System (IDRS) employee and network configuration information.

**Implementation Completed:** May 6, 2002

**Responsible Official**

Deputy Commissioner for Modernization & Chief Information Officer M  
Chief, Information Technology Services M:l  
Director, Enterprise Operations M:l:E

**Corrective Action Monitoring Plan**

During SACS disaster recovery testing, Systems Support Division and the Tennessee Computing Center (TCC) will verify that all Martinsburg Computing Center data and communications changes were removed from the SACS backup system at TCC.

# Management Advisory Report: The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements

---

Attachment

## **Management Response to Draft Management Advisory Report – “The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements” (#200220043)**

### **Recommendation #2**

The Chief, Information Technology Services, should ensure that future software and other configuration changes to the SACS backup mainframe computer at the TCC follow the SSD configuration management process.

### **Assessment of Cause**

The configuration of the non-production Security and Communication System (SACS) mainframe computer environment at the Tennessee Computing Center (TCC) is not compliant with IRS requirements, since the audit trail reporting capabilities were not enabled. The required configuration control board did not approve changes to the configuration of this backup mainframe as part of a disaster recovery conversion. As a result, we stopped further changes to the backup mainframe configuration, including implementation of audit trail reporting capabilities. Without these capabilities, any user actions originating on this backup mainframe computer would not be reported to management.

### **Corrective Action #2**

The Director Enterprise Operations will ensure future software and other configuration changes to the SACS backup mainframe computer at the TCC follow the Systems Support Division (SSD) configuration management process.

**Implementation Completed:** May 6, 2002

### **Responsible Official**

Deputy Commissioner for Modernization & Chief Information Officer M  
Chief, Information Technology Services M:I  
Director, Enterprise Operations M:I:E

### **Corrective Action Monitoring Plan**

Tennessee Computing Center, Martinsburg Computing Center and Systems Support Division will conduct regularly scheduled conference calls to monitor and discuss SACS related issues and projects. We will include any configuration change in the meeting agenda for review by all attendees.