



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

**March 30, 2010**

**Reference Number: 2010-20-028**

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.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

March 30, 2010

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER  
COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED  
DIVISION  
COMMISSIONER, WAGE AND INVESTMENT DIVISION

*Michael R. Phillips*

**FROM:** Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Additional Security Controls Are Needed to  
Protect the Automated Collection System (Audit # 200920012)

This report presents the results of our review of whether the Internal Revenue Service (IRS) has implemented access, audit trail, and configuration management<sup>1</sup> controls to secure the Automated Collection System (ACS). This audit addresses the IRS major management challenge of Security of information systems. The audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2009 Annual Audit Plan and was part of our statutory requirement to annually review the adequacy and security of IRS technology.

### *Impact on the Taxpayer*

The ACS is used to perform critical IRS processes such as collecting tax revenues and helping taxpayers resolve their tax issues. The IRS needs to implement additional security controls to protect the ACS and sensitive taxpayer data. The lack of complete security controls increases the risks that taxpayer data could be stolen or critical computer operations could be disrupted.

### *Synopsis*

The ACS is a telephone contact system used by IRS employees to collect unpaid taxes and secure tax returns from delinquent taxpayers who have not complied with previous collection notices. Specifically, the ACS allows employees to receive and initiate telephone calls; access

---

<sup>1</sup> See Appendix IV for a glossary of terms.



## *Additional Security Controls Are Needed to Protect the Automated Collection System*

taxpayers' account information; issue a variety of letter correspondence to taxpayers; review taxpayers' case histories; and issue notices, liens, or levies to resolve cases. The ACS plays a vital role in the IRS collection program. In Fiscal Year 2008, the ACS contributed to the collection of \$4.8 billion (17 percent) of the \$27.5 billion collected by the IRS Small Business/Self-Employed and Wage and Investment Divisions.

Because employees use the ACS to access sensitive taxpayer information, the IRS must implement strict access controls to limit employees' access privileges to only those privileges needed to perform assigned duties. IRS procedures also require that computer systems be configured to create audit trails to identify inappropriate and suspicious activities on the system. We found the IRS implemented several access controls. For example, the IRS configured the ACS to automatically disable user accounts that are inactive for 45 calendar days and delete user accounts that are inactive for 90 calendar days, separated key duties among ACS personnel to limit conflicts of interest, configured the ACS to automatically lock out users after three unsuccessful logon attempts, and implemented a session lockout control on employee workstations to prevent unauthorized users from gaining access to the ACS when the workstations are left unattended for a designated time period. However, the following required access controls have not been implemented.

1. None of the managers we interviewed perform a periodic review of their employees' access privileges to ensure the privileges are adequately restricted. The risk of users gaining unauthorized privileges on the ACS increases when managers do not periodically review their employees' access privileges. In addition, managers are not timely removing their employees' user account when the employee transfers to another IRS function. When access privileges are not promptly deleted from the system, opportunities exist for the employee to inappropriately access and modify taxpayer data.
2. Six of our sampled 109 employees' system privileges were not restricted to only those privileges needed to perform assigned duties. When users are granted excessive access privileges, the risk increases for malicious actions and unauthorized disclosure of taxpayer data. We also found some managers did not document their approval of their employees' access privileges in the IRS' Online 5081 system. When managers do not document their approval of employees' access privileges, there is an increased risk of employees obtaining greater privileges than needed.

IRS procedures also require the use of audit trails to detect unauthorized accesses and suspicious activities on computer systems. However, the IRS is not capturing all of the required auditable events in ACS audit trails. The IRS informed us that enabling all required auditing events would negatively affect system performance. In addition, the audit trail data were not protected from unauthorized modification. The IRS reported that it took corrective actions during our fieldwork and eliminated unneeded audit trail access privileges for 58 employees.



## *Additional Security Controls Are Needed to Protect the Automated Collection System*

In addition to implementing access and audit trail controls, the IRS must implement configuration management controls to manage the effects of changes in configurations on the ACS. Configuration management includes the management of security features and assurances through control of the changes made to hardware, software, and documentation throughout the life cycle of the system. The IRS developed a number of required configuration management policies, procedures, and guidance and established configuration control boards. It also uses an automated configuration policy checker program on a monthly basis to evaluate the ACSWeb<sup>2</sup> server configuration settings. However, basic configuration management controls have not been implemented.

1. The IRS had not developed an overall configuration management plan for the ACS.
2. The IRS had not documented and maintained a complete, accurate inventory of the ACS hardware, software, and document configuration items.
3. Changes to ACSWeb software configuration items are not properly documented, tested, and authorized.

The IRS did not timely correct high- and medium-risk system vulnerabilities that it identified on the ACSWeb servers using the automated configuration policy checker program.

### *Recommendations*

To improve access controls on the ACS, the Chief Technology Officer should: 1) make the current efforts to enhance or replace the Online 5081 system a top priority and 2) instruct the Modernization and Information Technology Services organization's ACS Applications Development office to create call site procedures to clarify the capabilities of each user profile at the Resource Access Control Facility (RACF®) and ACS application level. Also, the Commissioner, Small Business/Self-Employed Division, should request that the ACS Application Development office reinstate the ACS Security Maintenance Report that identifies changes to employees' access levels for the ACS application. Lastly, the Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should: 1) instruct ACS managers to review their employees access privileges on the RACF® and the ACS application during the annual Online 5081 recertification process, 2) instruct ACS managers to remove users' accounts from the ACS when the users transfer to non-ACS functions, and 3) immediately review the Online 5081 for all of their employees that need elevated RACF® privileges to ensure their approval is documented in the Online 5081.

---

<sup>2</sup> The ACSWeb component provides a web interface that allows communication with the mainframe computers.



## *Additional Security Controls Are Needed to Protect the Automated Collection System*

To improve configuration management on the ACS, the Chief Technology Officer should: 1) set completion dates and prioritize the work needed to complete the high level and ACS configuration management plans; 2) appoint an ACS configuration manager to oversee ACS configuration management activities; 3) direct the ACS configuration manager to protect critical ACS documentation by storing the documents in the DocIt system; 4) identify key software configuration items, assign unique identifiers, and maintain the items in the ClearCase® system to allow efficient monitoring; 5) ensure the IRS' required change management procedures are followed for all changes to the ACSWeb servers; and 6) establish criteria and completion dates for addressing vulnerabilities found on servers and compare the results of monthly vulnerability scans to verify that vulnerabilities are timely addressed.

### *Response*

IRS management agreed with 10 of our 12 recommendations and stated that some corrective actions have already been taken. The IRS disagreed with the wording of our recommendation for the Chief Technology Officer to instruct the ACS Applications Development office to create call site procedures and guidelines to clarify the capabilities of user profiles. The IRS stated the Chief Technology Officer does not have this authority to direct the actions of business units. However, the Chief Technology Officer agreed to work with the Director, Filing and Payment Compliance, Small Business/Self-Employed Division, to create the call site procedures and to clarify the capabilities of each user profile. The Director, Filing and Payment Compliance, will ensure the user profile information is included in the appropriate call site training.

The IRS also disagreed with our recommendation to appoint an ACS configuration manager to oversee key ACS configuration management activities. The IRS stated the Applications Development ACS team is aligning with current configuration management procedures to implement corrective actions related to software and documentation repositories, transmittal procedures, and version control. Management's complete response to the draft report is included as Appendix VI.

### *Office of Audit Comment*

We concur with the IRS' corrective actions to update and clarify the ACS call site procedures for users' profiles and ensure user profile information is included in call site training, but we disagree with the decision to not appoint an ACS configuration manager to oversee key ACS configuration management activities, which could prevent the IRS from addressing the weaknesses we reported. However, we believe the corrective actions to the other 11 recommendations will sufficiently mitigate this particular weakness. As such, no further action is required at this time.



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

*Table of Contents*

**Background** .....Page 1

**Results of Review** .....Page 3

    Several Access Controls Have Been Implemented, but Additional  
    Controls Are Needed for the Call Site Employees .....Page 3

Recommendations 1 through 3:.....Page 6

Recommendation 4:.....Page 7

Recommendation 5:.....Page 8

Recommendation 6:.....Page 9

    Audit Trail Controls for the Automated Collection System  
    Were Not Operating Effectively .....Page 10

    Basic Configuration Management Practices Have Not Been  
    Implemented to Protect the Automated Collection System.....Page 11

Recommendations 7 and 8: .....Page 13

Recommendations 9 and 10: .....Page 15

Recommendation 11: .....Page 16

Recommendation 12: .....Page 17

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 18

    Appendix II – Major Contributors to This Report .....Page 21

    Appendix III – Report Distribution List .....Page 22

    Appendix IV – Glossary of Terms.....Page 23

    Appendix V – Process to Obtain Access to  
    the Automated Collection System .....Page 26

    Appendix VI – Management’s Response to the Draft Report .....Page 27



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

*Abbreviations*

ACS	Automated Collection System
IRS	Internal Revenue Service
OL5081	Online 5081
RACF®	Resource Access Control Facility



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

## *Background*

The Automated Collection System (ACS) is a telephone contact system used by Internal Revenue Service (IRS) employees to collect unpaid taxes and secure tax returns from delinquent taxpayers who have not complied with previous collection notices. Specifically, the ACS allows employees to receive and initiate telephone calls; access taxpayers' account information; issue a variety of letter correspondence to taxpayers; review taxpayers' case histories; and issue notices, liens, or levies to resolve the cases. The ACS plays a vital role in the IRS collection program. In Fiscal Year 2008, the ACS contributed to the collection of \$4.8 billion (17 percent) of the \$27.5 billion by the IRS Small Business/Self-Employed<sup>1</sup> and Wage and Investment Divisions. In addition, each nonmanagerial ACS employee collected an average \$1.49 million in Fiscal Year 2007. The two IRS business units that primarily use the ACS, the Small Business/Self-Employed and Wage and Investment Divisions, listed the recovery of the ACS as a top priority in resuming critical IRS business processes after a disaster or emergency incident.

***The ACS program collected \$4.7 billion in Fiscal Year 2008 and is critical to IRS collection and customer service efforts.***

The ACS is a three-tiered system. The first tier is the mainframe computerized inventory system that controls and maintains the Integrated Data Retrieval System balance due and nonfiler cases that are worked by ACS employees. The Integrated Data Retrieval System operates in the computing centers in Memphis, Tennessee, and Martinsburg, West Virginia. The second tier of the ACS includes the ACSWeb servers that are located in the computing center in Memphis, Tennessee. The ACSWeb provides the web interface that allows communication with the mainframe. The third tier includes the workstations that employees use to access the ACSWeb servers and conduct collection activities.

The ACS is used by approximately 5,500 employees in 14 call sites around the nation. For many taxpayers, a customer service representative in an ACS call site is the first personal contact with the IRS. In order to do their job, these employees have access to a large amount of sensitive taxpayer data on the ACS. These data include the taxpayer's name; home address; date of birth; telephone numbers; Taxpayer Identification Number; account information relating to tax liabilities; information regarding liens, levies, assets, partnerships, and/or corporation names; and the power of attorney's personal information. ACS employees also have access to personal information of a taxpayer's spouse.

---

<sup>1</sup> See Appendix IV for a glossary of terms.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

Federal legislation and IRS policy require that taxpayer information be protected from malicious actions and unauthorized access or modification. In addition, the Federal Government has long recognized that the greatest harm to computer systems has come from authorized individuals engaged in improper activities, whether intentional or accidental.<sup>2</sup> Insider threats are often disgruntled employees who believe the business, institution, or agency has treated them unfairly and feel justified in taking malicious actions. To minimize these threats, the IRS developed security controls to prevent, limit, and detect unauthorized access to its computer systems.

For example, access to systems should be based on the concept of “least privilege.” Least privilege, which is one of the most basic principles for securing computer resources, means that employees should be granted only those access rights and privileges that they need to perform their duties. In addition, audit trail controls should be implemented to detect unlawful and unauthorized activities on computer systems. The IRS is required to capture, analyze, and retain audit trails. The IRS must also implement configuration management controls to establish and maintain the integrity and reliability of ACS hardware, software, and documentation. Configuration management is critical to manage the vulnerabilities of the ACS and reduce the potential for exploitation by inside and outside hackers.

We focused this security review of the ACS on access, audit trail, and configuration management controls. The review was performed at the call sites in Jacksonville, Florida; Philadelphia, Pennsylvania; and Ogden, Utah; the computing centers in Memphis, Tennessee, and Martinsburg, West Virginia; and the offices of the Modernization and Information Technology Services organization and Small Business/Self-Employed Division in New Carrollton, Maryland, and Washington, D.C. We performed this review during the period March through September 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

<sup>2</sup> Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III – *Security of Federal Automated Information Resources*, November 28, 2000.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

*Results of Review*

**Several Access Controls Have Been Implemented, but Additional Controls Are Needed for the Call Site Employees**

The IRS uses the Resource Access Control Facility (RACF®) to control access to the mainframe computer systems that maintain the balance due and nonfiler tax accounts that are worked by ACS employees. A RACF® security administrator assigns the ACS employee one of three user account profiles: operator, manager, or security representative. The manager and security representative profiles allow elevated privileges. For example, the manager profile allows managers to unlock employees' accounts and the security representative profile allows security representatives to unlock managers' accounts. Users with a manager or security representative profile also have the ability to use a query tool to view large amounts of sensitive taxpayer collection data.

After granting an employee a RACF® profile, the RACF® security administrator notifies the employee's call site security representative, who assigns the employee one of eight profiles on the ACS application. This second level of application-specific privileges controls the employee's activities on the ACS application to ensure the employee can perform only their assigned duties. Examples of the ACS application profiles include National Office,<sup>3</sup> Master, Supervisor, and Operator. An employee could have more than one profile on the ACS application, and the ACS application profiles allow different privileges than those granted by the RACF®.

To manage user access accounts on IRS computer systems, employees and managers are required to use the Online 5081 (OL5081) system. Using the OL5081 system is the IRS' approved method for adding, updating, and removing users and their system privileges on all IRS systems. The ACS employee completes his or her access request on the system, and the manager approves the request. If the employee needs elevated RACF privileges, the manager documents his or her approval in the special instructions section of the employees' OL5081 request. However, the OL5081 does not document managerial approval of the ACS application privileges. Appendix V provides an overview flowchart of the process to gain access to the ACS.

---

<sup>3</sup> The National Office profile on the ACS application is the highest profile with the most elevated privileges.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

### **Several access controls have been implemented**

We identified several ACS access controls that were operating effectively.

- User accounts that have no activity for 45 calendar days are automatically disabled and user accounts that have no activity after 90 calendar days are automatically deleted. Disabling and deleting inactive accounts is crucial because the existence and availability of inactive accounts increase the risks of unauthorized access and disclosure of taxpayer data and the potential for malicious actions or misuse by individuals such as former employees who no longer have a need to know or others who may obtain access by posing as those individuals.
- Duties were properly separated to limit conflicts of interest among key ACS personnel. For example, security representatives at the call sites cannot change RACF® privileges, which are controlled by the RACF® security administrators in IRS campuses. Individuals who review the audit logs are separate from the individuals who enable user access and privileges. The 24 application developers, with detailed knowledge of the system design and vulnerabilities, do not have access to the ACS production system. In addition, ACS managers who authorize user access using the OL5081 system cannot add users to the system or enable access privileges.
- The automatic system lockout control properly locks out users after three unsuccessful logon attempts.
- A session lock control was implemented on ACS workstations to prevent unauthorized users from gaining access to information when the workstation is left unattended after a designated time period.
- An appropriate warning banner is displayed when accessing the ACS to warn all persons attempting to gain access to the system that the system and its information are for authorized use only and that attempts to illegally log on to the system could lead to criminal prosecution.
- Lastly, effective controls were implemented to prevent the existence of duplicate, default, and shared accounts on the ACS. These accounts offer unauthorized users additional opportunities to access the system and have been properly deleted from the system.

While the IRS has implemented several access controls, some required controls have not been implemented. For instance, none of the managers we interviewed perform a periodic review of their employees' access privileges to ensure the employees have only those system privileges needed to perform official duties, some managers did not timely remove their employees' system accounts when the employees transferred to other IRS functions, users' system privileges were not always based on the principle of least privilege, and some managers did not document their approval of their employees' RACF® privileges in the OL5081 system.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

**ACS managers were not reviewing their employees' access privileges**

ACS managers are required to annually review the appropriateness of their employees' access accounts and account privileges using the OL5081 system. Managers should ensure that users need an ACS access account and that the related account privileges are based on the employees' need to know and job duties. Our interviews with 14 managers in the Jacksonville call site and 27 managers in the Philadelphia call site determined that, although managers annually review their employees on the OL5081 system to ensure the employees' ACS accounts are still needed, none of the managers review the OL5081 system to determine the appropriateness of the employees' access privileges.

During our interviews, ACS managers were not aware of the requirement to review their employees' RACF® or ACS application privileges. In addition, the OL5081 system was not designed with the functionality needed to facilitate managers' review of employees' access privileges. For example, during the annual OL5081 recertification process, the special instructions section of the OL5081 system is not accessible from the recertification screens that are displayed on managers' computers. The OL5081 system also lacks the functionality to document the employees' ACS application privileges. Therefore, when a manager seeks to increase an employee's access privileges on the ACS application, the manager uses informal methods such as email or verbal communication to notify the local call site security representatives. These informal methods provide no official written record of manager authorization for employee access privileges to the ACS application.

The IRS has initiated actions to resolve the lack of OL5081 system functionality. The Modernization and Information Technology Services organization's Cybersecurity office has started gathering requirements to implement a new identity and access management<sup>4</sup> system, which will address weaknesses with the OL5081 system. The requirements gathering work was scheduled to be completed in December 2009. After that work is complete, the Cybersecurity office will make recommendations to either enhance the OL5081 system or replace it with a commercial off-the-shelf software product.

We also found that the IRS discontinued a critical ACS Security Maintenance Report for the ACS application in Calendar Year 2002. This report identified changes to employees' access privileges on the ACS application. Managers could review the report to detect unauthorized changes to employees' privileges on the ACS application. However, the report was discontinued because it was not considered useful. We believe the report could be used to manage ACS user privileges.

The risk of users gaining unauthorized privileges on the ACS application increases when managers do not periodically review their employees' access privileges. A RACF® security

---

<sup>4</sup> Identity and access management is the gatekeeper mechanism that guards access to systems, applications, and data and represents the first line of defense protecting the confidentiality, integrity, and availability of data.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

administrator or a call site security representative could give employees unauthorized elevated privileges without being detected. The employees could then have inappropriate access to view sensitive taxpayer data or make adjustments to collection cases.

## **Recommendations**

**Recommendation 1:** The Commissioner, Small Business/Self-Employed Division, should request the Modernization and Information Technology Services organization's ACS Application Development office reinstate the ACS Security Maintenance Report that identifies changes to employees' access levels for the application. The report should be reviewed by managers on a monthly basis to ensure that the employees have the correct access privileges on the ACS application.

**Management's Response:** The IRS agreed with this recommendation. The Small Business/Self Employed Division will coordinate with ACS Modernization and Information Technology Services organization staff to reinstate this report. The ACS call sites have been instructed that this report will be reinstated and should be monitored on a monthly basis to ensure that employees have the proper privileges on the ACS.

**Recommendation 2:** The Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should instruct ACS managers to review their employees' RACF® access privileges during the annual OL5081 recertification process to ensure the privileges are authorized and follow the principle of least privilege. Until the IRS enhances or replaces the OL5081 system, managers should also review their employees' ACS access privileges on the ACS application.

**Management's Response:** The IRS agreed with this recommendation. The Small Business/Self Employed and Wage and Investment Divisions are finalizing managerial guidance on reviewing and updating employee access privileges during the OL5081 recertification process and on the ACS application. Additional collaboration is needed with all stakeholders prior to implementation.

**Recommendation 3:** The Chief Technology Officer should make the identity access provisioning and management solution to enhance the OL5081 system or acquire a commercial off-the-shelf software product a top priority. The new system should document managers' access authorizations for the RACF® and ACS application.

**Management's Response:** The IRS agreed with this recommendation. The Chief Technology Officer has made identity and access management a priority. The Internal Identity and Access Management Program has been established as a governed program with allocated funding and dedicated staff. Phase 4 of the program will commence in December 2011.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

### **Managers are not timely initiating actions to remove employees' system access when the employees no longer have a need to access the ACS**

Although most of the 181 user accounts in our sample<sup>5</sup> were needed and being used by current ACS employees, 4 of the user accounts belonged to former ACS employees who had transferred to another IRS function. For all four cases, the managers had not taken action to remove the users' accounts. The accounts remained on the system for 1 to 3 months subsequent to the employees' transfers.

ACS managers are responsible for using the OL5081 system to promptly notify the officials responsible for removing access accounts when an employee leaves the IRS, is reassigned to other duties, is on extended leave, or is under disciplinary action. All accounts should be removed within 1 week of an individual's departure on friendly terms and immediately upon an individual's departure on unfriendly terms.

Managers we interviewed were unsure of the procedures regarding employee transfers and removal of access privileges. Managers also mistakenly believed the gaining manager is responsible for removing employee access accounts.

### ***Recommendation***

**Recommendation 4:** The Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should instruct the ACS managers to remove users from the ACS by updating the employee's OL5081 profile if the employee leaves the IRS, is reassigned to a non-ACS function, is on extended leave, or is under disciplinary actions.

**Management's Response:** The IRS agreed with this recommendation. The Wage and Investment and Small Business/Self-Employed Divisions are finalizing managerial guidance on reviewing and updating employee access privileges during the OL5081 recertification and on the ACS application, and will issue a memorandum to all managers regarding current procedures.

### **Users' privileges were not always based on the principle of least privilege**

IRS procedures require employees' system privileges be restricted to only those needed to perform their duties. Most of the 109 employees in our sample with elevated privileges had the appropriate level of access. However, six did not need their elevated privileges to perform their duties.

- Four employees were managers who needed the security representative privileges on the RACF® to unlock users' accounts. However, the managers were also given security representative privileges on the ACS application because the managers mistakenly

---

<sup>5</sup> See Appendix I for sample methodology.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

thought the elevated privileges on the RACF® require corresponding privileges on the ACS application. We believe the managers gained the unneeded excessive privileges on the ACS application due to the lack of written procedures or guidelines explaining the differences between RACF® and ACS application profiles.

- Two employees with manager privileges on the RACF® were not authorized to have them. One of the employees also had manager privileges on the ACS application. The employees' managers informed us the employees' prior managers granted the employees elevated privileges for a temporary work detail. However, when the detail was over, the privileges were not revoked.

The security representative privileges given to the above four managers on the ACS application provided the managers with elevated privileges such as the ability to increase the privileges of other users. The manager privileges on the RACF® that were given to the two employees included the ability to perform management queries to view large amounts of sensitive tax collection data. When users are granted access permissions beyond their assigned responsibilities, the risks of malicious actions and unauthorized disclosure of taxpayer data are increased.

### ***Recommendation***

***Recommendation 5:*** The Chief Technology Officer should instruct the ACS Applications Development office to create call site procedures and guidelines to clarify the capabilities of each user profile at the RACF® and ACS application levels. The procedures and guidelines should be incorporated into call site training and emphasize the IRS requirement to ensure users are given only those access privileges needed to perform assigned duties.

***Management's Response:*** The IRS disagreed with this recommendation as written and stated that the Chief Technology Officer does not have the authority to direct the actions of the business units and, likewise, the heads of the business units do not have the authority to direct the actions of the Chief Technology Officer. However, the Chief Technology Officer agreed to work with the Director, Filing and Payment Compliance, Small Business/Self-Employed Division, to create call site procedures and guidelines to clarify the capabilities of each user profile at the RACF® and ACS application levels. The Chief Technology Officer will provide the required user profile information and the Director, Filing and Payment Compliance, will ensure the user profile information is included in the appropriate call site training.

***Office of Audit Comment:*** We concur with the IRS' alternative action to create call site procedures to clarify the capabilities of each user profile at the RACF® and ACS application levels and to ensure the user profile information is included in the appropriate call site training.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

**ACS managers did not document their approval of employees' elevated RACF® access privileges in the OL5081 system**

ACS managers are required to document their approval of employees' elevated access privileges in the special instructions section of the OL5081 system. Without documentation of access privileges, accountability for granting access cannot be readily determined and the risk of employees gaining more access than needed is increased.

ACS managers did not document in the OL5081 system their approval of elevated RACF® privileges for 46 of the 109 ACS users in our sample that had elevated access privileges. The managers informed us that these 46 employees needed the elevated privileges, but the managers did not take the necessary actions to approve the privileges in the OL5081 system.

- 28 employees had a hardcopy access request that was converted into electronic format when the OL5081 system was implemented in July 2002. However, after the hardcopy documents were converted to the OL5081 system, managers did not carry out their responsibility to ensure their approval of the employee's elevated privileges was also documented.
- 16 employees without a manager approval in the OL5081 system had no document trail for us to determine how they received elevated privileges. We believe managers bypassed the OL5081 system and used unofficial methods to request higher access privileges for their employees. Since the managers do not have the ability to actually grant the privileges on the RACF®, we believe the RACF® administrators granted the elevated access without requiring proper OL5081 authorization from the managers.
- 2 employees were temporarily authorized by their managers to have a security representative profile for a 120-day detail. However, when the detail ended, the managers did not revoke the privileges. The managers informed us that the employees are currently approved to have the elevated privileges, but the managers did not use the OL5081 system to document their approval.

The lack of control increases the risk of malicious actions on the ACS and unauthorized disclosure of taxpayer data.

***Recommendation***

**Recommendation 6:** The Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should instruct all ACS managers to immediately review the OL5081 system for all of their employees that need elevated RACF® privileges to ensure the manager's approval is documented in the employees' OL5081 profile.

**Management's Response:** The IRS agreed with this recommendation. The Wage and Investment and the Small Business/Self-Employed Divisions will direct the call sites



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

to document managerial approval on all elevated RACF® privileges as reflected on the OL5081 system. In addition, both operating divisions have included this security issue in their Fiscal Year 2010 Operational Review Plans.

### ***Audit Trail Controls for the Automated Collection System Were Not Operating Effectively***

#### ***The ACS was not capturing the required auditable events***

IRS procedures require that computer systems be configured to create audit trails to identify inappropriate and suspicious activity on the system. The ACS mainframe database uses Native DB2<sup>6</sup> auditing to track the activities of database administrator accounts. However, Native DB2 auditing of the ACS database is not logging all required events that would allow IRS security officials to detect suspicious activities. For example, database administrator access to taxpayer data in the ACS database is rarely logged. We found that 87 percent of the ACS database tables did not have auditing enabled to track database administrators' accesses to taxpayer data.

The IRS informed us that enabling the required auditing would negatively affect system performance. However, when these required auditing controls are not implemented, the risk of not detecting suspicious activities, including unauthorized access to taxpayer data and misuse by privileged users, increases.

#### ***Recommendation***

Recommendations will be provided in the audit report for the *Review of Enterprise Audit Trails Management* (Treasury Inspector General for Tax Administration Audit #200820003).

#### ***ACS audit trails were not adequately protected from unauthorized modification***

IRS procedures require that an annual review of user accounts and profiles shall be performed to ensure compliance with the principle of least privilege. Access to audit trail files should be limited to only those users that need some level of access to perform their duties.

We found 61 employees have ALTER access to the ACS application audit trail. However, our initial testing found that several of these employees did not need this elevated access privilege. The excessive privilege was given to the employees because the RACF® group permissions are too broad. The group permission granted access to not only the ACS application audit trail but to other datasets as well. Employees who needed access to the other datasets did not need ALTER access to the ACS application audit trail.

---

<sup>6</sup> Native DB2 auditing is part of the IBM database management system that IBM developed for its mainframe computer system.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

The RACF® security administrator agreed to review the access privileges of all 61 employees and eliminate the unneeded employee access by creating a specific group profile.

Users with the ALTER access authority could create, modify, or delete the audit trails either accidentally or intentionally to conceal unauthorized activity, thereby compromising the integrity of the audit trail. Consequently, unauthorized access to the system could occur without detection.

***Management Actions:*** Prior to the completion of our fieldwork, IRS officials reported they took corrective actions to eliminate the unneeded access to the ACS audit trails. The IRS reported that current ALTER access is now limited to only three users that need this access privilege to perform their assigned duties.

### ***Basic Configuration Management Practices Have Not Been Implemented to Protect the Automated Collection System***

To manage the effects of changes in configurations on the ACS, the IRS must implement basic configuration management controls. Configuration management includes the management of security features and assurances through the control of changes made to hardware, software, and documentation throughout the life cycle of the system. All configuration management activities fall within the following four primary functions.

- **Identification** – Identifying those items whose configuration needs to be controlled, usually consisting of hardware, software, and documentation. These key items are referred to as configuration items.
- **Change Control** – Establishing procedures for proposing or requesting changes to the configuration items. Change control procedures include evaluating the changes for desirability, obtaining authorization for changes, publishing and tracking changes, and implementing changes. This function also identifies those persons and organizations that have authority to make the changes, and those that make up the configuration control boards.
- **Status Accounting** – Maintaining formal records of established configurations and making regular reports of configuration status.
- **Auditing** – Performing regular evaluation of the configuration, where the physical and functional configuration is compared to the documented configuration.

The IRS has developed a number of required configuration management policies, procedures, and guidance and established configuration control boards. In addition, it uses an automated scanner on a monthly basis to evaluate the ACSWeb server configurations. However, basic configuration management controls have not been implemented. Specifically, the IRS did not:



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

- Develop an overall Configuration Management Plan for the ACS.
- Document and maintain a complete accurate inventory of the ACS hardware, software, and document configuration items.
- Properly document, test, and authorize changes to ACSWeb software configuration items.
- Timely correct security vulnerabilities on the ACSWeb servers.

### **The IRS did not develop an overall Configuration Management Plan for the ACS**

Configuration management begins with planning. IRS procedures require information system developers to create and implement a written configuration management plan. Guidance for creating the plan is provided by the National Institute for Standards and Technology,<sup>7</sup> which recommends that the plan: 1) address roles, responsibilities, and configuration management processes and procedures; 2) define when in the system development life cycle the configuration items are placed under configuration management; 3) define the means for uniquely identifying configuration items; and 4) define the process for managing the configuration items.

The IRS has not completed a configuration management plan for the ACS. IRS officials informed us that the plan has not been completed because the IRS must first develop its higher level configuration management plans that lay the foundation of guidance, policies, and procedures that all organizations should follow to develop system-specific plans. However, the IRS has not established completion dates for these high level plans.

The lack of an ACS configuration management plan has prevented the IRS from appointing a configuration manager to control configuration management activities and serve as the focal point for ACS configuration management. As a result, key ACS hardware, software, and documentation have not been identified and documented in a configuration management plan. The IRS cannot effectively establish and maintain the integrity of the ACS configuration items and associated artifacts without this key plan. In addition, the IRS cannot adequately manage the security of the system and has limited assurance that changes to hardware, software, and document configuration items are being properly monitored.

### ***Recommendations***

Many of the configuration management issues we identified for the ACS should be addressed by the IRS at an enterprise level. We plan to conduct an enterprise configuration management review in Fiscal Year 2010 and will likely address many of the issues we identified for the ACS.

---

<sup>7</sup> National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations, Revision 3*.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

As such, we limited our recommendations in this report to the corrective actions that we believe the IRS should take immediately to improve configuration management for the ACS.

**Recommendation 7:** The Chief Technology Officer should set completion dates and prioritize the work needed to complete the high level and ACS configuration management plans.

**Management's Response:** The IRS agreed with this recommendation. The Applications Development Compliance Domain will complete a revised project level Configuration Management Plan.

**Recommendation 8:** The Chief Technology Officer should appoint an ACS configuration manager to oversee key ACS configuration management activities during the development of the IRS high level configuration management plans.

**Management's Response:** The IRS disagreed with this recommendation and stated that the Applications Development ACS team is aligning with current configuration management procedures to implement corrective actions related to software and documentation repositories, transmittal procedures, and version control.

**Office of Audit Comment:** We continue to believe the IRS should appoint an ACS configuration manager to strengthen the oversight of key ACS configuration management activities. The IRS decision to not appoint an ACS configuration manager could prevent the IRS from addressing the weaknesses we reported. However, we believe the corrective actions to the other 11 recommendations will sufficiently mitigate this particular weakness. As such, no further action is required at this time.

**The IRS has not documented and maintained a complete accurate inventory of the ACS hardware, software, and document configuration items**

As we stated earlier in this report, one of the functions of configuration management is to identify the key configuration items that need to be controlled. These items usually consist of hardware, software, and documentation. The identification process must be performed in accordance with project identification requirements that include the use of unique identifiers to allow the configuration items to be easily tracked and monitored. This process is the initial step in establishing the final baseline configuration for all configuration items and systems.

After identifying the key configuration items and assigning unique identifiers, the IRS must develop, document, and maintain an inventory of the system components that 1) accurately reflects the system, 2) is at the level of detail deemed necessary for tracking and reporting, and 3) includes information necessary to achieve effective property accountability.

We found the IRS has not documented and maintained the key ACS hardware, software, and documentation.



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

### *The ACS hardware is not adequately documented and maintained*

The information needed to identify, monitor, and track ACS hardware configuration items is not adequately documented and maintained. The IRS' official computer asset inventory system, the Information Technology Assets Management System, does not include required monitoring and tracking data, such as the network internet protocol address, function, interconnections, and system/component owners and project name. To locate ACS hardware in the Information Technology Assets Management System, IRS employees must find the identifying information from other IRS offices. Also, the IRS' inventory system does not allow employees to query the inventory system by a project or computer system's name. During our audit, we had to provide IRS employees the ACS hardware barcodes or serial numbers to enable the employees to query the inventory system and obtain a list of the ACSWeb servers. The user information for the servers was recorded in the inventory system as "Shared ITS" and the contact name for seven of the servers was recorded as "Shared, ITS."

Other issues identified in our inventory verification of the ACSWeb servers included the following discrepancies.

- The IRS provided us with multiple ACSWeb server inventory lists, each with incorrect information.
- Two of 10 ACSWeb servers in the Tennessee Computing Center had incorrect serial numbers recorded in the Information Technology Assets Management System.
- The Information Technology Assets Management System incorrectly reported five ACSWeb servers as "in use." However, the servers were not being used.

The IRS has not implemented adequate inventory policies and procedures. Although the IRS is in the process of updating inventory guidance to educate all employees on their responsibilities for inventory management, the inventory guidance has not been finalized. In addition, the Modernization and Information Technology Services organization's Enterprise Operations organization indicated that the inventory validation is inadequate because the employees who perform the inventory validation only scan the barcodes that are affixed to the hardware items. The employees do not verify that the required identifying information for each hardware item is properly recorded in the Information Technology Assets Management System.

### *Key ACS software configuration items are not adequately maintained*

The IRS uses the ClearCase® system to safeguard and control changes to critical ACS software. However, the IRS could not provide a list of key ACS software items under configuration control in the ClearCase® system. The ACS Applications Development office stated it could take several days to locate all the service packs, service files, custom files, software, and other ACS application software under configuration control in the ClearCase® system. We believe the inability to readily locate and provide ACS software configuration items stored in the ClearCase® system is due to the manner in which the items are labeled and stored. The key



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

software items should be identified, labeled, and stored in the ClearCase® system to facilitate efficient configuration management activities.

### *Some key ACS documentation is not adequately maintained*

Key ACS documentation should be maintained in the DocIt system, which is the IRS' enterprise web-based electronic document management system used to safeguard and control changes to critical project documentation. However, the DocIt system did not contain all key ACS documents, such as Enterprise Life Cycle documents and configuration management documents. Many key documents are stored on the IRS local area network file servers. The Applications Development office is using spreadsheets to track some critical documents. However, the spreadsheets showed numerous notes questioning whether documents are obsolete. Some of the key ACS documents are maintained on the local area network because the ACS Applications Development office is waiting for guidance from the Applications Development Division Coordinator.

When key hardware, software, and document configuration items are not identified, documented, and maintained, changes to those configuration items are difficult to track. In addition, when an accurate inventory of system components is not adequately maintained, the ability to detect the addition of unauthorized components or devices is affected.

## ***Recommendations***

**Recommendation 9:** Subsequent to the appointment of the new ACS configuration manager, the Chief Technology Officer should direct the ACS configuration manager to manage and protect critical system documentation from unauthorized changes by storing all critical ACS system documentation in the DocIt system.

**Management's Response:** The IRS agreed with moving the ACS application systems documentation under DocIt for configuration management purposes.

**Recommendation 10:** Subsequent to the appointment of the new ACS configuration manager, the Chief Technology Officer should direct the ACS configuration manager to identify the key software configuration items, assign unique identifiers, and maintain the items in the ClearCase® system to facilitate efficient tracking, monitoring, and other configuration management activities.

**Management's Response:** The IRS agreed with ensuring that all ACS software configuration items are tracked in the appropriate configuration management tool.

### **Changes to ACSWeb configuration items are not properly evaluated, tested, and authorized**

All changes to the ACS are required to be evaluated, tested, and approved. A formal change request document should be prepared and submitted to the appropriate change configuration



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

control board prior to the change being made to the system. After the configuration control board reviews and approves the change, a transmittal is sent to a system administrator requesting the change to be made.

We found the Server, Middleware, Test Systems Infrastructure office and the ACS Applications Development office sent a total of 23 transmittals to the system administrators from January to July 2009 requesting changes to the ACSWeb environment. A change request should have been prepared and submitted to the configuration control board for each of these 23 changes. However, only three change requests were prepared.

The IRS did not follow its own change management procedures. IRS officials who requested changes to the ACSWeb operating system and applications believed a change request document was not warranted for changes they considered to be routine. The IRS defined routine changes as those that would not cause a work stoppage or similar problem. In addition, we found that transmittals are often used to make changes to the system without going through the change request process. Transmittals that do not go through the change request process are not subjected to rigorous review and approval standards, and the IRS does not have adequate assurance that the changes will not affect the system's integrity, security, and functionality.

Changes to the ACS that are not properly evaluated, tested, and approved could circumvent security controls and undermine the reliability of the system.

### ***Recommendation***

**Recommendation 11:** The Chief Technology Officer should ensure the required change management procedures are followed for all changes to the ACSWeb.

**Management's Response:** The IRS agreed with this recommendation. The Applications Development Compliance Domain will follow accepted change management procedures outlined in the ACS Configuration Management Plan.

### **Security vulnerabilities on the ACSWeb servers were not timely corrected**

To maintain the security of the ACS, the IRS runs UNIX Policy Checker scans on the 15 ACSWeb servers each month to identify vulnerabilities that could be exploited by malicious users. A transmittal from the Server, Middleware, Test Systems Infrastructure office to the system administrator is required before the system administrator can correct some of the vulnerabilities. However, system administrators are permitted to correct some of the vulnerabilities without a transmittal.

The IRS is not timely addressing high- and medium-risk system vulnerabilities that it identifies on the ACSWeb servers. The IRS UNIX Policy Checker scans that the IRS ran on the servers from January through May 2009 reported that some high- and medium-risk vulnerabilities remained on ACSWeb servers for 2 to 5 months before system administrators took corrective



---

## *Additional Security Controls Are Needed to Protect the Automated Collection System*

---

actions. For example, 1 high-risk password vulnerability remained on the same 9 servers for 3 consecutive months, and the same 2 high-risk password vulnerabilities remained on all 15 servers for a minimum of 2 consecutive months. An average of 8 medium-risk vulnerabilities remained on the same four servers for 5 consecutive months.

Limited staffing resources may have contributed to the IRS not timely correcting the security vulnerabilities. The system administrators responsible for maintaining the ACSWeb servers are responsible for maintaining approximately 200 servers, and their work is affected by other management priorities, such as keeping the systems operating.

Another reason why the vulnerabilities are not timely corrected is because the IRS has not established clear criteria and deadlines for correcting vulnerabilities. IRS procedures state that vulnerabilities should be “promptly” corrected, but no time periods are provided in the procedures.

The risks to the ACS are increased when vulnerabilities are not timely corrected. We believe managing vulnerabilities of systems will reduce the potential for exploitation by insider and outside attackers and may involve less time and effort than responding after an exploit has occurred.

### ***Recommendation***

**Recommendation 12:** The Chief Technology Officer should revise IRS procedures to include specific criteria and deadlines for addressing vulnerabilities found on servers and compare the results of monthly vulnerability scans to verify that vulnerabilities are timely addressed.

**Management’s Response:** The IRS stated that, as of March 11, 2010, two activities are in place to address this recommendation. First, monthly configuration scans are performed on servers, which meet the Department of the Treasury’s enhanced controls standards. These scans are the basis for an enterprise-wide get well plan that addresses noncompliant systems agency-wide. Computer system owners and their staffs are currently being engaged on remediation efforts. Second, the security monitoring staff in the IRS’ Enterprise Operations organization has established a risk finding group to address the high risks associated with UNIX and Windows server platforms. Bi-weekly calls are held to discuss the corrective actions associated with the high risks identified. The security monitoring staff monitors and tracks the high risks and provides remediation status. The IRS stated these efforts have resulted in a 50 percent decrease in open high-risk findings from July to November 2009. The IRS will monitor the continuing effectiveness of these actions before revising or instituting new procedures or criteria.



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

**Appendix I**

*Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine whether the IRS has implemented access, audit trail, and configuration management controls to secure the ACS. To accomplish this objective, we:

- I. Determined whether key access controls are in place and operating effectively to limit access to only authorized users of the ACS by reviewing user access control account lists; interviewing ACS managers, security representatives, and systems administrators; and observing the access controls on users' workstations.
  - A. Determined whether the IRS properly managed ACS user accounts. To test ACS end user accounts, we obtained the control account list from the RACF<sup>1</sup> and selected a random sample of 102 accounts. We initially selected a random sample because we wanted each account to have an equal chance of being selected, and we wanted our sample to represent the population of ACS user accounts. We used the following sample plan:

	Operators	Managers	Security Representatives
Population Size	4,503	219	94
Confidence Level	95%	90%	90%
Error Rate	5%	2%	1%
Sample Size	72	20	10

After testing the 102 accounts, we sorted the control account list by call site and determined that a large number of employees in the Jacksonville and Philadelphia call sites had elevated privileges. Therefore, we tested the 66 managers and 13 security representatives in these 2 sites. Our total sample was 181 (102 + 66 + 13) accounts. The total number of users in our sample with elevated privileges was 109 (30 from the initial sample and 79 from the Jacksonville and Philadelphia call sites). We also tested all 20 of the system administrators' user accounts on the ACSWeb servers operating in the Tennessee Computing Center. We determined whether each user account was approved by the employee's manager in the OL5081 system and recertified within the last 12 months, whether any other account reviews were

<sup>1</sup> See Appendix IV for a glossary of terms.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

- performed, and whether the appropriate security officials were notified when access was no longer needed.
- B. Determined whether generic, default, duplicate, shared, or temporary accounts exist on the Tier II ACSWeb servers by reviewing the control lists of all user accounts on the servers.
  - C. Determined whether inactive accounts were disabled after 45 calendar days and deleted after 90 calendar days by reviewing the most current computer-generated access control list.
  - D. Determined whether user permissions were restricted based on the principle of least privilege by comparing the users' actual RACF privileges to those authorized on the OL5081 system.
  - E. Determined whether duties were adequately separated to limit conflicts of interest among key personnel by reviewing user access control lists and interviewing security personnel.
  - F. Interviewed system administrators to determine whether the system automatically locks out a user after three unsuccessful logon attempts.
  - G. Determined whether a session lock control has been implemented to prevent users from gaining access to unauthorized information when a workstation is left unattended after a designated time period. We had a user and a system administrator demonstrate this control to determine that it was operating.
  - H. Determined whether remote and wireless access to the ACS is allowed by interviewing system administrators and reviewing the System Security Plan.
  - I. Determined whether the ACS and ACSWeb display the appropriate warning banner to warn all persons attempting to gain access to the system that the system and its information are for authorized use only. We observed this control on users' workstations.
- II. Determined whether the IRS is capturing the required audit events in the audit trails and protecting the audit trails from unauthorized modification by coordinating with the Washington D.C. audit group performing a concurrent review<sup>2</sup> of enterprise audit trail controls.
- III. Evaluated the configuration management controls over the ACS by interviewing key IRS information technology officials; reviewing applicable Internal Revenue Manual and Law

---

<sup>2</sup> *Review of Enterprise Audit Trails Management* (Treasury Inspector General for Tax Administration Audit #200920003).



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Enforcement Manual procedures; and reviewing hardware, software, and documentation configuration items.

- A. Evaluated the ACS Configuration Management Plan to determine whether the hardware, software, and documentation items that require configuration control are defined and that the plan addresses roles, responsibilities, and configuration management procedures.
- B. Determined whether baseline configurations have been documented and maintained for each of the hardware and software components.
- C. Determined whether changes to configuration items are documented and authorized before changes are made.
- D. Determined whether physical and logical access restrictions are defined and implemented to control changes to the configuration items, and whether access records to the computer room and software libraries are maintained.
- E. Determined whether configuration changes are continuously monitored, including modifications and upgrades, to verify the changes were applied correctly.
- F. Determined whether the IRS reviews ACS hardware and software to identify and eliminate unnecessary functions, ports, protocols, and/or services.
- G. Determined whether an inventory of ACS components is documented and maintained that accurately reflects the system.

**Internal controls methodology**

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: ACS access, audit trail, and configuration management internal controls. We evaluated these internal controls by interviewing management, reviewing ACS users' accounts and system privileges, and reviewing supporting documentation.



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

**Appendix II**

*Major Contributors to This Report*

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Allen Gray, Audit Manager  
Richard Borst, Senior Auditor  
Cari Fogle, Senior Auditor  
George Franklin, Senior Auditor  
Bret Hunter, Senior Auditor  
Thomas Nacinovich, Senior Auditor  
Esther Wilson, Senior Auditor



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Commissioner for Services and Enforcement SE  
Deputy Commissioner, Small Business/Self-Employed Division SE:S  
Deputy Commissioner, Wage and Investment Division SE:W  
Associate Chief Information Officer, Applications Development OS:CTO:AD  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaisons:  
    Commissioner, Small Business/Self-Employed Division SE:S  
    Commissioner, Wage and Investment Division SE:W  
    Director, Program Oversight OS:CIO:SM:PO



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

**Appendix IV**

*Glossary of Terms*

<b>Term</b>	<b>Definition</b>
ALTER (Access Authority)	Allows users to read, update, move, rename, and delete audit log data.
Audit Trail or Log	A record showing who has accessed a system and what operations the user has performed during a given period.
Balance Due Account	An unpaid taxpayer account. Also referred to as a Taxpayer Delinquent Account.
Baseline	A specified set of documents, software, and other items defined as final (or point-in-time) products for a project.
Change Request	The medium for requesting approval to change a baselined product or other controlled item.
ClearCase®	Rational ClearCase® was developed by the IBM corporation. This product provides version control and software configuration management.
Configuration Control Board	A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items and for ensuring implementation of approved changes.
Configuration Item	Any component of the Information Technology infrastructure that falls under the control of the configuration management process.
Configuration Management	Involves establishing proper control over approved project documentation, hardware, and software and assuring changes are authorized, controlled, and tracked.
Configuration Management Plan	Establishes and documents the requirements, standards, practices, and procedures for configuration management. The process of completing the configuration management plan includes defining <i>baselines</i> and establishing the labeling scheme for configuration items.



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

Enterprise Life Cycle	Establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensures alignment with the overall business strategy.
Information Technology Assets Management System	The official IRS computer equipment database used to record all computer inventories.
Integrated Data Retrieval System	An IRS computer system capable of retrieving or updating stored information. This system works in conjunction with a taxpayer's account records.
Nonfiler Case	An unfiled tax return for a taxpayer. Also referred to as a Taxpayer Delinquency Investigation.
Online 5081 (OL5081)	Virtually every customer within the IRS must utilize the IRS Form 5081, Information System User Registration/Change Request, to request access to information systems and applications. The OL5081 system replaces the paper Form 5081 with an automated, standard process. It provides automated submission, approval, recertification, and filing of the Form 5081 on an enterprise-wide basis.
Patch	A quick repair job for a piece of programming. Sometimes called a "fix."
Query Management Facility	A tool for performing queries on the mainframe database to retrieve large amounts of taxpayer collection data.
Resource Access Control Facility	A security software sold by the IBM Corporation to manage access controls and auditing for the IBM mainframe computer systems.
Small Business/Self-Employed Division	Serves fully and partially self-employed individuals and small businesses. The Division also has responsibility for taxpayers filing estate and gift, employment, excise, and international tax returns.
System Development Life Cycle	A conceptual model used in project management that describes the stages involved in an information systems development project, from an initial feasibility study through maintenance of the completed application.



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

Transmittal	For this audit report, the purpose of a transmittal is to either document changes that the Tier II Support Services has made to the operating system or database (whether it is a configuration change or a patch) or to initiate action by field personnel (usually a systems administrator) for applying patches, making required configuration changes, and installing software.
UNIX Policy Checker	An application that validates the operating system security configuration of Solaris computers to IRS policy.
Vulnerability	In computer security, a security risk or weakness which allows an attacker to reduce a system's Information Assurance.
Wage and Investment Division	Serves taxpayers whose only income is derived from wages and investments.
Web or Application Services	Services (usually including some combination of programming and data, but possibly including human resources as well) that are made available from a business' web server for web users or other web-connected programs.

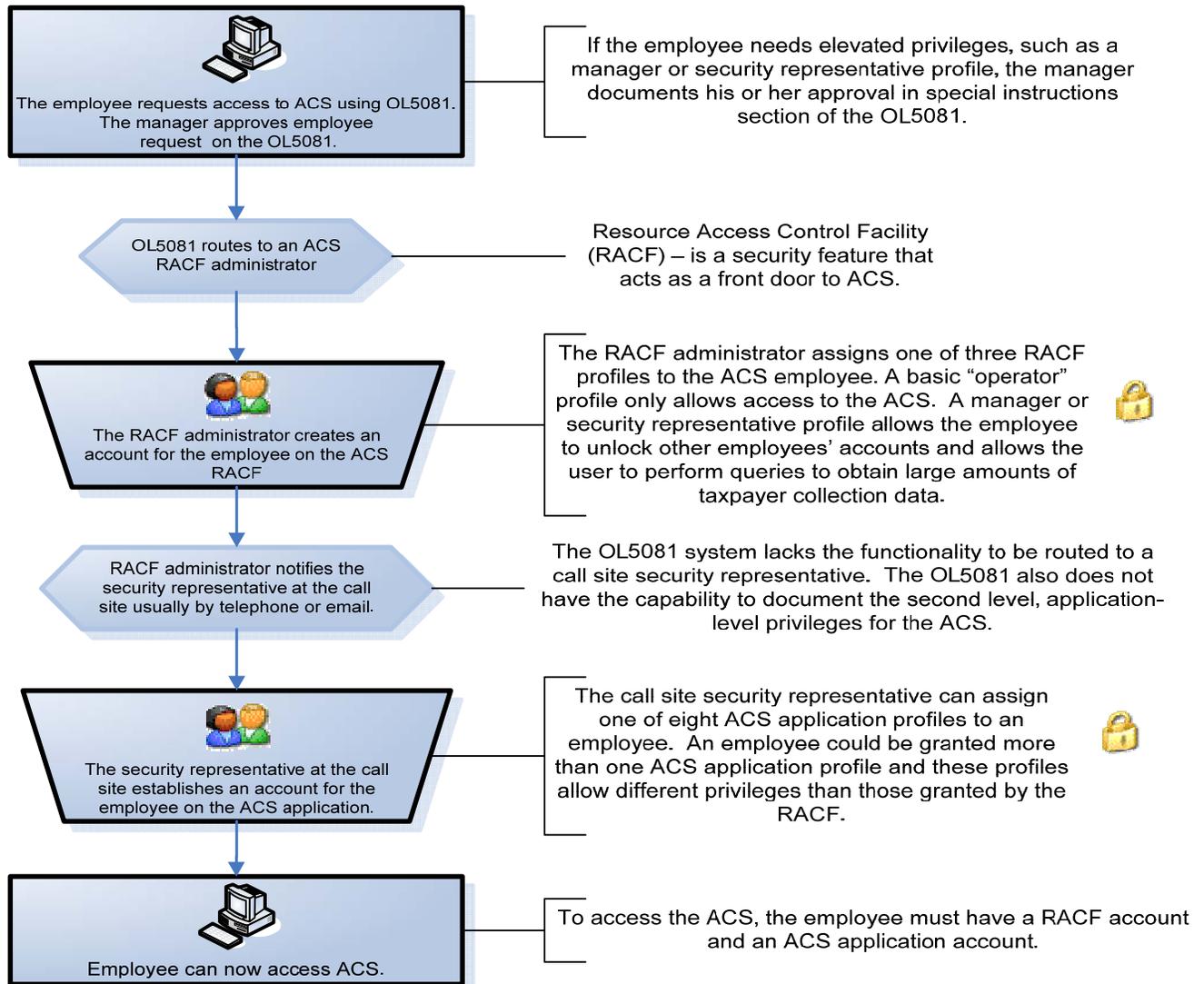


*Additional Security Controls Are Needed to Protect the Automated Collection System*

**Appendix V**

*Process to Obtain Access to the Automated Collection System*

IRS employees must be granted two levels of access to use the ACS. Access must be granted on the RACF® and on the ACS application.





*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

**Appendix VI**

*Management's Response to the Draft Report*



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

**RECEIVED**  
MAR 17 2010  
BY: *DRB*

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Miltholland *Terence V. Miltholland*  
Chief Technology Officer

SUBJECT: Draft Audit Report – Additional Security Controls Are Needed to  
Protect the Automated Collection System (Audit #200920012)  
(i-trak #2010-71806)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate the report recognizing that the Internal Revenue Service (IRS) has implemented several access controls to ensure the Automated Collection System (ACS) is operating effectively:

- Configured ACS to automatically disable user accounts that are inactive for 45 calendar days and delete user accounts inactive for 90 calendar days;
- Separated key duties among ACS personnel to limit conflicts of interest;
- Configured ACS to automatically lock out users after three unsuccessful logon attempts; and
- Implemented a session lockout control on employee workstations to prevent unauthorized users from gaining access to the ACS when the workstations are left unattended for a designated time period.

The IRS' Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes; your recommendations will further improve our security posture. The attachment to this memo details our planned corrective actions to the recommendations.

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Agnes Spruill at (202) 283-7018.

Attachment



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated Collection System (Audit # 200920012) (i-trak # 2010-71806)

---

**RECOMMENDATION #1:** The Commissioner, Small Business/Self-Employed Division, should request the Modernization and Information Technology Services organization's ACS Application Development office reinstate the ACS Security Maintenance Report that identifies changes to employees' access levels for the application. The report should be reviewed by managers on a monthly basis to ensure that the employees have the correct access privileges on the ACS application.

**CORRECTIVE ACTION #1:** We agree with this recommendation. The Small Business/Self Employed Division will coordinate with the ACS MITS staff to reinstate this report. We have instructed our sites that this report will be reinstated and should be monitored on a monthly basis to ensure that employees have the proper privileges on the ACS system.

**IMPLEMENTATION DATE:** May 15, 2010

**RESPONSIBLE OFFICIAL:** Director, Filing & Payment Compliance (Small Business/Self/Employed)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #2:** The Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should instruct ACS managers to review their employees' RACF® access privileges during the annual OL5081 recertification process to ensure the privileges are authorized and follow the principle of least privilege. Until the IRS enhances or replaces the OL5081 system, managers should also review their employees' ACS access privileges on the ACS application.

**CORRECTIVE ACTION #2:** We agree with this recommendation. The Wage and Investment Division and Small Business/Self Employed are finalizing managerial guidance on reviewing and updating employee access privileges during the OL5081 recertification process and on the ACS application. Additional collaboration is needed with all stakeholders prior to implementation.

**IMPLEMENTATION DATE:** May 15, 2010

**RESPONSIBLE OFFICIALS:**  
Director, Filing & Payment Compliance (Wage and Investment Division)  
Director, Filing & Payment Compliance (Small Business/Self Employed)



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated Collection System (Audit # 200920012) (i-trak # 2010-71806)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #3:** The Chief Technology Officer should make the identity access provisioning and management solution to enhance the OL5081 system or acquire a commercial off-the-shelf software product a top priority. The new system should document managers' access authorizations for the RACF® and ACS application.

**CORRECTIVE ACTION #3:** We agree with this recommendation. The Chief Technology Officer has made Identity and Access Management a priority. The Internal Identity and Access Management Program have been established as a governed program, with allocated funding and dedicated staff. The identity access provisioning and management solution is a part of Phase 4 of the overall program. Phase 4, the Provisioning and Management solution, will commence December 2011.

**IMPLEMENTATION DATE:** December 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #4:** The Commissioners, Small Business/Self-Employed and Wage and Investment Divisions, should instruct the ACS managers to remove users from the ACS by updating the employee's OL5081 profile if the employee leaves the IRS, is reassigned to a non-ACS function, is on extended leave, or is under disciplinary actions.

**CORRECTIVE ACTION #4:** We agree with this recommendation. The Wage and Investment Division and Small Business/Self Employed are finalizing managerial guidance on reviewing and updating employee access privileges during the OL5081 recertification process and on the ACS application, and will issue a memo to all managers regarding current procedures.

**IMPLEMENTATION DATE:** May 15, 2010

**RESPONSIBLE OFFICIALS:**  
Director, Filing & Payment Compliance (Wage and Investment Division)  
Director, Filing & Payment Compliance (Small Business/Self Employed)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated Collection System (Audit # 200920012) (i-trak # 2010-71806)

---

**RECOMMENDATION #5:** The Chief Technology Officer should instruct the ACS Applications Development office to create call site procedures and guidelines to clarify the capabilities of each user profile at the RACF® and ACS application levels. The procedures and guidelines should be incorporated into call site training and emphasize the IRS requirement to ensure users are given only those access privileges needed to perform assigned duties.

**CORRECTIVE ACTION #5:** We disagree with this recommendation as written. Within the IRS, the Chief Technology Officer does not have the authority to direct the actions of the business units. Similarly, the heads of the business units do not have the authority to direct the actions of the Chief Technology Officer. The recommendation requires that specific IT organizations under the Chief Technology Officer create user profile information that is to be included in ACS call site training for managers. In the IRS, responsibility for creating and delivering ACS training is with the Director, Filing & Payment Compliance (Small Business/Self Employed). The recommendation as written does not reflect the collaboration between the Chief Technology Officer and business units that is necessary to implement the actions you suggest.

The Chief Technology Officer agrees to work collaboratively with the Director, Filing & Payment Compliance (Small Business/Self Employed) to create call site procedures and guidelines to clarify the capabilities of each user profile at the RACF® and ACS application levels. The Chief Technology Officer organization will provide the required user profile information to be included in the appropriate call site training. The Director, Filing & Payment Compliance (Small Business/Self Employed) will ensure that the user profile information is included in the appropriate call site training.

**IMPLEMENTATION DATE:** September 1, 2010

**RESPONSIBLE OFFICIAL:**

Director, Filing & Payment Compliance (Small Business/Self Employed)  
Chief Technology Officer (via the ACIO, Enterprise Operations and ACIO, Applications Development) as co-owners

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #6:** The Commissioners, SBSE, and W&I Division, should instruct all ACS managers to immediately review the OL5081 system for all of their employees that need elevated Resource Access Control Facility (RACF)® privileges to ensure the manager's approval is documented in the employees' OL5081 profile.

**CORRECTIVE ACTION #6:** We agree with this recommendation. The Wage and Investment Division and Small Business/Self Employed will direct the sites to document managerial



*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated Collection System (Audit # 200920012) (i-trak # 2010-71806)

approval on all elevated RACF privileges as reflected in the OL5081 system. Additionally, both operating divisions have included this security issue in their FY 2010 Operational Review Plans.

**IMPLEMENTATION DATE:** May 15, 2010

**RESPONSIBLE OFFICIALS:**

Director, Filing & Payment Compliance (Wage and Investment Division)  
Director, Filing & Payment Compliance (Small Business/Self Employed)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #7:** The Chief Technology Officer should set completion dates and prioritize the work needed to complete the high level and ACS configuration management plans.

**CORRECTIVE ACTION #7:** We agree with this recommendation. The AD Compliance Domain will complete a revised project level Configuration Management Plan.

**IMPLEMENTATION DATE:** January 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development (Compliance Domain)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #8:** The Chief Technology Officer should appoint an ACS configuration manager to oversee key ACS configuration management activities during the development of the IRS high level configuration management plans.

**CORRECTIVE ACTION #8:** We disagree with this recommendation. The AD ACS team is aligning with current procedures, as indicated in IRM 2.27.1, "Configuration Management, Configuration Management," to implement corrective actions related to software, and documentation repositories, transmittal procedures and version control.

**IMPLEMENTATION DATE:** N/A

**RESPONSIBLE OFFICIAL:** N/A

**CORRECTIVE ACTION MONITORING PLAN:** N/A



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated Collection System (Audit # 200920012) (i-trak # 2010-71806)

---

**RECOMMENDATION #9:** Subsequent to the appointment of the new ACS Configuration Manager, the Chief Technology Officer should direct the ACS Configuration Manager to manage and protect critical system documentation from unauthorized changes by storing all critical ACS system documentation in the DocIt system.

**CORRECTIVE ACTION #9:** We agree with moving the ACS application systems documentation under DocIT for configuration management purposes.

**IMPLEMENTATION DATE:** January 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development (Compliance Domain)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #10:** Subsequent to the appointment of the new ACS Configuration Manager, the Chief Technology Officer should direct the ACS Configuration Manager to identify the key software configuration items, assign unique identifiers, and maintain the items in the ClearCase<sup>®</sup> system to facilitate efficient tracking, monitoring, and other configuration management activities.

**CORRECTIVE ACTION #10:** We agree with ensuring that all ACS software configuration items are tracked in the appropriate configuration management tool.

**IMPLEMENTATION DATE:** January 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development (Compliance Domain)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #11:** The Chief Technology Officer should ensure the required change management procedures are followed for all changes to the ACSWeb.

**CORRECTIVE ACTION #11:** We agree with this recommendation. The AD Compliance Domain will follow accepted change management procedures outlined in the ACS Configuration Management Plan.



---

*Additional Security Controls Are Needed to  
Protect the Automated Collection System*

---

Attachment

Draft Audit Report – Additional Security Controls Are Needed to Protect the Automated  
Collection System (Audit # 200920012) (i-trak # 2010-71806)

---

**IMPLEMENTATION DATE:** January 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development  
(Compliance Domain)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into  
the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis  
until completion.

**RECOMMENDATION #12:** The Chief Technology Officer should revise IRS procedures to  
include specific criteria and deadlines for addressing vulnerabilities found on servers and  
compare the results of monthly vulnerability scans to verify that vulnerabilities are timely  
addressed.

**CORRECTIVE ACTION #12:** This action is closed. IRS has in place two activities which  
address the concerns expressed in the recommendation. (1) Monthly configuration scans to meet  
Treasury CVM 9 enhanced controls are the basis for an enterprise get-wall plan that addresses  
non-compliant systems agency wide and is currently engaging the systems owners and their  
staffs on remediation efforts. (2) Enterprise Operations security monitoring staff has established  
a risk finding group to address the high risks associated with UNIX and Windows server  
platforms. Bi-weekly calls are held with divisional POCs to discuss corrective actions for the  
high risks identified. They monitor and track the high risks and provide remediation status data  
via their share Point site. As a result of these activities there has been an approximate 50%  
reduction in open high-risk findings from July, 2009 to November, 2009. IRS will monitor the  
continuing effectiveness of these actions before revising or instituting new procedures or criteria.

**IMPLEMENTATION DATE:** March 11, 2010

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into  
the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis  
until completion.