TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Access Controls for the Automated Insolvency System Need Improvement

May 16, 2011

Reference Number: 2011-20-046

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.

Redaction Legend:
1 = Tax Return/Return Information
3(d) = Identifying Information

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

ACCESS CONTROLS FOR THE AUTOMATED INSOLVENCY SYSTEM NEED IMPROVEMENT

Highlights

Final Report issued on May 16, 2011

Highlights of Reference Number: 2011-20-046 to the Internal Revenue Service Commissioner for the Small Business/Self-Employed Division and the Chief Technology Officer.

IMPACT ON TAXPAYERS

Bankruptcy petitions filed in Federal courts were up 32 percent in Calendar Year 2009 compared to Calendar Year 2008. The Internal Revenue Service (IRS) receives notification of a bankruptcy case because taxpayers are required to list their creditors and liabilities when filing for bankruptcy protection. The IRS inputs the taxpayers' sensitive information into its Automated Insolvency System (AIS) to track the legal requirements for dealing with the taxpayers and to protect the Government's financial interest. Unauthorized access to the AIS could jeopardize taxpayers' legal rights.

WHY TIGTA DID THE AUDIT

This audit was initiated because the Small Business/Self-Employed Division requested that TIGTA review the AIS access controls. The objective of the review was to determine whether the IRS implemented access controls for the AIS to protect taxpayers' personal data and to ensure the Government's interest is protected when taxpayers file for bankruptcy.

WHAT TIGTA FOUND

Although some AIS access controls are in place, such as the automatic lockout control and password complexity settings, other required access controls have not been implemented or are not operating effectively.

TIGTA found many IRS employees have excessive privileges on the AIS. The excessive privileges are due to two primary reasons. First, managers did not ensure duties were adequately segregated among employees to prevent and detect unauthorized activities. The second reason is due to the inadequate role-based access control scheme that was developed for the AIS. The inadequate access control scheme causes managers to inadvertently grant unneeded, excessive AIS privileges to employees.

TIGTA also found IRS managers and user administrators were not following the requirement to use the Online 5081 system to authorize and revoke access to the AIS. In addition, some significant actions taken on bankruptcy cases are not logged and reported in the AIS Manager Review screen to allow managers to detect errors and inappropriate activities.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, Small Business/Self-Employed Division, 1) identify incompatible duties and implement policies to segregate those duties; 2) issue a memorandum to Insolvency office managers requiring them to adhere to the new policy when assigning duties and approving AIS access rights; 3) define and document user requirements for the AIS based on employee job functions and position descriptions and submit these requirements to the Applications Development office in a formal work request; and 4) issue a memorandum to managers emphasizing the requirement to use the Online 5081 system to authorize, revoke, and review employees' AIS access authorizations.

TIGTA also recommended that the Associate Chief Information Officer, Applications Development, 1) ensure application developers have read-only access to the AIS, 2) develop software to systemically create and assign passwords for new AIS users, and 3) create a role-based access control scheme for the AIS.

The IRS agreed with the recommendations and stated it had already taken two corrective actions. The IRS initiated a work request to develop a self-service password reset and auto generation feature for the AIS, and the User Administrator privilege was removed from the Developer privilege level.

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

May 16, 2011

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED
DIVISION
CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Access Controls for the Automated Insolvency System Need Improvement (Audit # 201020022)

This report presents the results of our review of the Automated Insolvency System. The overall objective of this review was to determine whether the Internal Revenue Service (IRS) implemented access controls for the Automated Insolvency System to protect taxpayers' personal data and to ensure the Government's interest is protected when taxpayers file for bankruptcy. This review was requested by the IRS's Small Business/Self-Employed Division and was included in the Treasury Inspector General for Tax Administration Fiscal Year 2010 Annual Audit Plan. This review addresses the major management challenge of Security of the IRS.

Management's complete response to the draft report is included as Appendix VI.

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 R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

Table of Contents

Appendices

Abbreviations

AIS	Automated Insolvency System
ENS	Electronic Notice System
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services
SB/SE	Small Business/Self-Employed

Background

Bankruptcy petitions filed in Federal courts were up 32 percent in Calendar Year 2009 compared to Calendar Year 2008.[1] This increase followed a 29 percent increase in bankruptcies from Calendar Year 2007 to Calendar Year 2008. If a bankruptcy petitioner has unpaid Federal taxes, the Internal Revenue Service (IRS) will receive notification of a bankruptcy petition from 1 of 86 Federal bankruptcy courts around the Nation because the taxpayer is required to list all liabilities when filing for bankruptcy protection. The IRS inputs the bankruptcy information into its Automated Insolvency System (AIS), which is the primary system used to protect the Government's financial interest in the bankruptcy case and the taxpayer's legal rights.

The AIS processes, stores, and transmits taxpayers' Personally Identifiable Information as well as their tax and financial data. It also interfaces with other bankruptcy subsystems and processes. Examples include:

- The Insolvency Interface Program is a subsystem that automates the transfer of AIS data to and from the Integrated Data Retrieval System[2] and, when necessary, prevents other IRS systems from sending collection notices to taxpayers.
- The Automated Discharge System is a subsystem that accesses Integrated Data Retrieval System information and takes the appropriate actions to discharge and close the cases.
- The Automated Proof of Claim System is a subsystem to prepare a Proof of Claim document detailing the Government's interest in the bankruptcy case.
- The Electronic Notice System (ENS) is a process that transfers new bankruptcy case information from United States Bankruptcy Courts into the AIS. The ENS notice informs the IRS that a taxpayer with a Federal tax liability has entered into a bankruptcy proceeding.

The Small Business/Self-Employed (SB/SE) Division's Collection Policy office owns the AIS and establishes and oversees policy for the Insolvency program. This program includes approximately 1,160 employees whose AIS access privileges and levels should be assigned based on their job responsibilities. For example, employees in the Centralized Insolvency Operation office[3] are given access privileges on the AIS that allow them to 1) add, update, and close bankruptcy cases on the system; 2) resolve upfront processing issues such as potentially

[1] Figures obtained from the Administrative Office of the United States Courts.
[2] See Appendix V for a glossary of terms.
[3] The SB/SE Division's Centralized Insolvency Operation office is part of the Campus Compliance Services' Filing and Payment Compliance office.

invalid Taxpayer Identification Numbers; and 3) identify collection activity that could violate Bankruptcy code provisions.

Other bankruptcy cases with complex issues are referred to Field Insolvency office employees, who are located in nine Territories throughout the country and are part of the Collection function's Advisory, Insolvency, and Quality program. These employees prepare the Proof of Claim, which is filed with the court to protect the Government's financial interest, and ensure taxpayers accurately list assets in their bankruptcy schedules.

In addition to the Insolvency program employees who access the AIS, approximately 340 non-Insolvency program employees use the system. These employees work in business units such as the Office of Appeals, Taxpayer Advocate, and Examination functions and primarily need view-only access.

In November 2008, the Modernization and Information Technology Services (MITS) organization Applications Development office upgraded the AIS from 34 Informix databases to a centralized Oracle database. The upgrade increased the AIS users' access to all bankruptcy data across the Nation, a capability needed by many managers and employees we interviewed.

Like its other systems that process or store sensitive data, the IRS must comply with Federal legislation and IRS procedures that require taxpayer information to be protected from malicious actions and inadvertent 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.[4] Insider threats are often disgruntled employees who believe the business or agency has treated them unfairly and feel justified in taking malicious actions. To minimize these threats, the IRS requires access controls be implemented for its computer systems to prevent, limit, and detect unauthorized access. For example, IRS procedures require access to systems be based on the concept of "least privilege."

Access controls must be implemented for computer systems based on the concept of "least privilege," which requires employees be given the minimum access privileges needed to perform their duties.

The Commissioner, SB/SE Division, requested the Treasury Inspector General for Tax Administration review the access controls for the AIS in Fiscal Year 2010. We focused our review on the access controls that were implemented to protect the privacy of taxpayer's data and reduce the potential for system exploitation. The review was performed at the IRS's Centralized Insolvency Operation office in the Campus office in Philadelphia, Pennsylvania; the Field Insolvency offices in Dallas, Texas, and Oakland, California; the MITS organization's

[4] Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III – Security of Federal Automated Information Resources, November 28, 2000.

Applications Development office in Indianapolis, Indiana; the Computing Center in Memphis, Tennessee; and the SB/SE Division Headquarters in New Carrollton, Maryland, during the period March through October 2010. 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 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.

Results of Review

Some Access Controls Have Been Implemented to Protect Taxpayers' Data and the Government's Interest in Bankruptcy Petitions

The IRS established some access controls in the AIS to protect the taxpayers' data and the Government's interest in bankruptcy cases. Examples include:

- A system automatic lockout control disables an AIS user's account after three unsuccessful login attempts. This control prevents a hacker from repeatedly trying to guess a user's password.
- The password settings comply with the IRS's password complexity requirements.
- The system displays the required banner to warn unauthorized users that the system is for authorized users only.
- Direct access to the Oracle database, which is part of the AIS, has been properly restricted. Only the database administrators have direct access to the database.

In addition, the Centralized Insolvency Operation office implemented a control to detect improper ENS notice deletions. The control requires a Centralized Insolvency Operation office manager to manually review all ENS notice deletions to ensure the deletions were warranted. Although this detective control improves security and our tests found no improper deletions, the control is labor intensive. The recommendations in this report will limit employee access to the ENS, prevent unauthorized employees from deleting ENS notices, and eliminate the need for this labor-intensive control.

Although some access controls are in place, we found other access controls have not been implemented or are not operating effectively.

Employees Have Excessive Privileges on the Automated Insolvency System

Employees have excessive privileges on the AIS due to two primary reasons. First, managers did not ensure duties were adequately segregated among employees to prevent and detect unauthorized activities. We found duties assigned to employees that cause a conflict of interest and violate the IRS's security requirement to ensure duties are adequately segregated among different employees to detect errors and fraud.

The second reason for employees' excessive AIS privileges is due to the inadequate role-based access control scheme that was developed for the AIS, which is presented in Figure 1. The IRS created the same four general access levels used in the previous Informix-based AIS and four new special access levels when it converted the system into its Oracle-based version.

We did not find errors or indications of fraud during our review. However, the excessive privileges on the AIS increase the risks that errors, fraud, or unauthorized activities could be performed by employees acting alone or in collusion with other employees.

Figure 1: General Access Levels and Special Access Levels

General Access	Privileges
Level 1	Users can 1) query and view the case data; 2) update and delete case data; 3) perform bulk processes such as printing notices and letters to taxpayers; 4) assign cases to employees; 5) view most AIS reports; 6) use support menus to view information such as the attorney/trustee data, employee data, and interest rates; and 7) access the ENS.
Level 2	Users can 1) query and view the case data, 2) update and delete case data, 3) perform bulk processes such as printing notices and letters to taxpayers, 4) view some AIS reports, and 5) access the ENS.
Level 3	Users can 1) query and view the case data, 2) update and delete case data, 3) access some reports, and 4) access the ENS.
Level 4	Users can query and view the case information.
Special Access	**Privileges**
Manager	Users can 1) view and print Manager reports, 2) access the Manager Support Menu to modify attorney/trustee data and employee data and perform bulk case assignments to employees, and 3) view the Manager Review screen to identify case actions taken by employees.
Analyst	Users can update and delete data in the support tables, such as the interest rates charged to delinquent tax debts.
User Administrator	Users can add new users to the system, assign privileges, unlock user access accounts, and create passwords.
Developer	Users can view a menu with 17 options to diagnose interface problems the AIS encounters with other systems. One of the options allows the user to add users to the AIS and assign privileges.

Source: AIS User Guide and Centralized Insolvency Operation office Senior Technical Advisor.

Duties are not adequately separated among employees to prevent and detect unauthorized activities

The National Institute for Standards and Technology[5] recommends, and IRS procedures require, that duties be adequately separated among employees to ensure no employee has the authority and system privilege to disrupt or corrupt a security process or computer system. However, some IRS officials assign additional duties to managers and employees that, when combined with the manager or employee's official duties and AIS privileges, violate the separation of duties requirement and increase the risks of errors or fraud. Examples include:

- Twelve Field Insolvency office managers whose duties include authorizing their employees' AIS access accounts using the Online 5081 (OL5081) system[6] were assigned the collateral duties of adding users to the system, enabling privileges, unlocking users' access accounts, and changing employees' privileges when the employees are temporarily promoted or transferred to another position. The User Administrator privileges that the managers gained to perform these duties violate the IRS's separation of duties policy. The critical security processes of authorizing and enabling access to a system must be separated among different employees to reduce the risk of errors and fraud. Field Insolvency office officials assigned these incompatible duties to a few managers in each Territory for the convenience of having a local user administrator.

- Field Insolvency office secretaries are responsible for performing administrative tasks, such as printing forms and letters to taxpayers and printing reports for managers. However, 3 of the 63 Field Insolvency office secretaries had the User Administrator privilege level because managers wanted the secretaries to unlock users' passwords. The security process of unlocking passwords is the responsibility of a trained user administrator and these highly sensitive privileges should be restricted to only a few employees.

- Field bankruptcy specialists work the bankruptcy cases assigned to them and represent the IRS in court. They are responsible for updating bankruptcy case information in the AIS, including the payment history. To perform these duties, the specialists need Access Level 2. However, we found four specialists were assigned duties that required the User Administrator privileges, which allow the specialists to create new users and assign privileges to the users. Specialists should not be assigned User Administrator duties because the specialist could assign excessive privileges to employees or create phantom users and then login as the phantom user to perform malicious actions in the AIS.

[5] National Institute for Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations, Revision 3.*

[6] The OL5081 is the official IRS system for requesting the establishment or cancellation of user accounts on all IRS systems.

- 114 employees had the AIS privilege to grant other users access to 2 AIS subsystems, the Insolvency Interface Program and the Automated Discharge System. These employees included Field bankruptcy specialists, revenue officers, Centralized Insolvency Operation office clerks, and policy analysts. Although these employees would first have to be granted access from the subsystem's system administrator, the duty of assigning access privileges should not be given to these types of employees because they have other duties and AIS privileges that pose a conflict of interest. Further, the duty of assigning access privileges should be given only to user administrators.

- The official duties of the system analyst in the Centralized Insolvency Operation office are to help employees and managers that incur problems with the AIS application and assign case inventory to managers. To perform these duties, the system analyst needs Access Level 1 and Manager privileges. However, this employee was also assigned the additional duties of adding new users to the AIS and changing users' privileges when employees separate from the IRS or change job functions. These additional duties require the system analyst to have the User Administrator privileges which, when combined with his or her Access Level 1 and Manager privileges, violates the IRS's separation of duties policy. The system analyst can update and delete case information including ENS notices, access Manager Reports, change key case information using the Manager privileges, add new users, assign privileges, and assign passwords. IRS procedures state that a user administrator shall have no more capability than appropriate to establish a user on a system or to establish a user within an application.

The Government Accountability Office's internal control standards for Government agencies[7] require agencies to identify incompatible duties and implement policies to segregate those duties. However, the IRS has not completed these critical actions for Centralized Insolvency Operation office or Field Insolvency office employees. We believe most managers assigned employees the previously noted incompatible duties because they were unaware of the separation of duties requirement and which key duties should be segregated. Nine of the 10 managers we interviewed indicated they believe secretaries should have the same privileges as managers. In addition, 3 of the 10 managers were unaware of their employees' AIS privileges.

Although the IRS has not identified incompatible duties for its Insolvency program employees, the IRS has completed this identification for application developers in the MITS organization. IRS procedures require application developers be given read-only access on the production system and should not have duties or privileges that would allow them to alter a production system. This requirement is due to their detailed knowledge of the system's security vulnerabilities and to ensure configuration changes to the system are approved and controlled. Application developers are responsible for developing and testing system changes in the development environment. Other employees in the MITS organization Enterprise Operations

[7] *Standards for Internal Controls in the Federal Government,* (GAO/AIMD-00-21.3.1, November 1999).

office are responsible for implementing the changes on the production system. However, we found 11 AIS application developers were assigned duties on the production system and had excessive privileges.

- The AIS Applications Development office manager informed us that 3 of the 11 developers do not need access to the AIS. The developers were given these privileges to help convert users to the new Oracle-based system. However, after the users were converted, the access privileges for the three application developers were not revoked.
- We determined most privileges included in the special Developer privilege level allow the developer read-only access to diagnose and troubleshoot interface problems that the AIS encounters with other systems. However, the eight developers who were assigned troubleshooting duties also had Access Level 1 and Manager privileges, which exceeded necessary read-only capabilities.
- Five of the 11 developers were also given User Administrator privileges that allow them to add users to the AIS, elevate users' privileges, and perform other powerful activities on the production AIS.

The AIS Applications Development office manager requested developers be given Access Level 1, Manager, and the User Administrator privileges to ensure they had all privileges necessary to troubleshoot users' problems with the system. The live data in the production AIS could not be replicated in the development and test environment to which the developers were limited. In addition, the AIS application developers informed us that other technical employees in the MITS organization, such as the systems administrators and database administrators, do not have sufficient AIS knowledge to troubleshoot and diagnose the AIS's interface problems.

Assigning employees duties that should be segregated among different employees increases the security risks and could lead to errors or malicious activities. Users can manipulate case data for their own personal gain or erroneously alter information that affects the IRS's ability to protect the Government's interest in bankruptcy cases.

A role-based access control scheme was not adequately implemented for the AIS

IRS procedures require access privileges to a system be based on a role-based access control scheme. This security requirement allows the IRS to create system roles for various job functions such as Field bankruptcy specialist and Field Insolvency office secretary. The privileges needed to perform the jobs should be assigned to the roles based on the concept of "least privilege." User administrators should then assign the appropriate role to the employee/user. A role-based access control scheme aligns employees' duties with system privileges and helps prevent errors and fraud.

We identified approximately 22 different job functions in the Centralized Insolvency Operation office and Field Insolvency offices. However, the AIS Applications Development office created only four general access levels and four special privilege levels for the AIS, as presented previously in Figure 1. This access control scheme does not adequately allow managers to align users' job duties with their AIS privileges and causes managers to inadvertently grant unneeded, excessive privileges to employees. The following are examples of excessive privileges gained by some employees. Additional examples are summarized in Appendix IV.

- Bankruptcy specialists in the Centralized Insolvency Operation office's Operations Support group investigate and assign a petitioning taxpayer's tax obligations to the non-petitioning spouse, when applicable. These employees also need the ability to view and change case information and determine which employee took which specific actions on a case. To perform these duties, the bankruptcy specialist needs Access Level 1 and Manager privileges. However, along with the needed privileges in Access Level 1, this access level gives the specialists unneeded, excessive privileges, such as the ability to perform bulk processes (e.g., printing notices and letters to taxpayers), change taxpayer payment data using the Payments screen, and delete ENS bankruptcy notices. The specialist also gains unneeded Manager privileges such as the capability to change the employee data and perform bulk case assignments.

- The Automated Processing Control Lead employees in the Centralized Insolvency Operations office need Access Level 1 and Manager privileges to reassign cases using the Case Assignment Guide, delete ENS notices, and review their group's work using the Manager Review screen. However, these employees also gain unneeded privileges with Access Level 1, such as access privileges to the Payments screen and bulk processes. They also gain unneeded access with their Manager privileges such as the capability to change attorney/trustee data and employee data.

- Managers' responsibilities include reviewing their employees' work on the AIS, modifying the case grade and proof required fields, accessing and printing manager reports, and authorizing employees' AIS access using the OL5081 system. However, the Manager privileges also include the privilege to elevate the access levels of AIS users, including their own access level. The privilege to modify the access level of a user should not be included in the Manager privileges because it conflicts with the managers' duty to authorize users' access to the system. This privilege to modify users' access privileges should be granted to user administrators.

- Field Insolvency office secretaries are responsible for administrative tasks such as printing forms and letters to taxpayers and printing reports for managers. However, 52 of the 63 secretaries had access to the AIS's Automated Proof of Claim subsystem. Five of the eight managers we interviewed stated they wanted the secretary to print reports from this subsystem. The Program Analyst for the Automated Proof of Claim subsystem confirmed that printing reports is the most common reason for granting secretaries access. However, the employees also gained the excessive privilege to modify the data in the system. Modifying case information is the job of a trained Insolvency employee, such as a Field bankruptcy specialist. The secretaries could purposely or erroneously change the Proof of Claim data.

- The User Administrator privileges include the right to create a password for a new access account. This right makes the User Administrator privilege level a significant security risk because user administrators have the capability not only to create an access account and assign high-level privileges, but also to create a password for the new account. The user administrator could create an account and password and then use the password to login to the AIS and perform malicious actions. The duty and system privilege of creating a password should be separated from the duty of creating an access account to ensure no one employee has the authority and system privilege to corrupt the security process of adding new users to the system. We found 30 employees have the User Administrator privileges. The AIS Applications Development office was instructed by the MITS organization Enterprise Operations office to create the User Administrator privileges to allow the SB/SE Division employees the capability to establish new end users on the system.

The AIS Applications Development office manager informed us that, during the 2008 AIS conversion process, the MITS organization Cybersecurity office directed the conversion be completed quickly and to keep the new system similar to the previous Informix-based system. The AIS application developers followed this guidance by implementing the same four general access controls that were used for the previous AIS and adding the four new special privilege levels. The application developers also informed us they were unaware of the IRS's role-based access control requirement.

In addition to any excessive privileges previously mentioned, the employees' excessive privileges could allow them to inadvertently or maliciously modify or delete the taxpayers' data in the AIS or perform other unauthorized actions. These actions could prevent the IRS from protecting the Government's financial interest in bankruptcy proceedings. *****3(d)********
******************3(d)***
****
****
****
****
*********************3(d)************************* **********1******************
1**********************************
**************************1**************** *******3(d)*************************
3(d)*********************************
****
***.

Management Actions: Subsequent to completing our fieldwork, we determined changes were made to the Access Level 1 and Manager privileges. Access to the Case Assignment Guide was removed from Access Level 1 and the right to modify users' access levels was removed from the Manager privileges. We acknowledge both of these changes to the access control scheme improve security. However, the AIS application developers did not provide evidence to support that these alterations to the AIS were tested, approved, and made by authorized employees. IRS configuration control procedures require changes to a production system be documented and approved using a formal Transmittal document.

In addition, the IRS informed us it removed the User Administrator privilege from the Developer privilege level after we completed our fieldwork. We did not verify this corrective action.

Recommendations

Recommendation 1: To ensure key duties and system privileges are adequately separated, the Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, SB/SE Division, should 1) identify incompatible duties and implement policies to segregate those duties, 2) issue a memorandum to Insolvency program managers requiring them to adhere to the new policy when assigning duties and approving AIS access privileges, and 3) designate a limited number of employees to perform the User Administrator duties. These employees should have no more capability than necessary to establish a user on the AIS.

> ***Management's Response:*** The IRS agreed with this recommendation. A role-based access control system is currently being developed which will define the roles of users and designate specific access privileges to the users' defined AIS profiles. Once this process is established, a memorandum will be issued to all managers requiring them to adhere to the new policy regarding segregation of duties. In addition, the Collection Policy office and the MITS organization are reprogramming the AIS to allow users to reset their passwords as opposed to the current process in which a user administrator must reset passwords. This corrective action would dramatically reduce the number of user administrators needed.

Recommendation 2: The Associate Chief Information Officer, Applications Development, should 1) remove the access account of the three application developers who are not assigned AIS troubleshooting duties, 2) remove the Access Level 1 and Manager privileges for the eight developers who are assigned troubleshooting duties and ensure they have only the Developer privileges and read-only access, 3) remove the User Administrator privilege level for the five developers who are assigned troubleshooting duties, and 4) develop a software product to systemically create and assign passwords for new AIS users.

> ***Management's Response:*** The Applications Development office generally agreed with this recommendation. The Applications Development office will ensure that access to the AIS is limited to personnel assigned AIS troubleshooting duties. In addition, Access Level 1 and Manager privileges will be retained for the developers who are

assigned troubleshooting duties until the role-based access control scheme is implemented. These privileges must be retained as-is until a role-based access control scheme is implemented which will allow the developers read-only access to these processes. Otherwise, developers lose troubleshooting and maintenance capabilities for these processes. The IRS will remove the User Administrator privilege level for the five developers who are assigned AIS troubleshooting duties. Finally, a work request has been input to request development of a self-service password reset and auto generation feature for the AIS.

Recommendation 3: The Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, SB/SE Division, should coordinate with the MITS organization Applications Development office to define and document user requirements for AIS users based on employee job functions and position descriptions, such as Field Insolvency office secretary and Centralized Insolvency Operation office automated processing control clerk. The new user requirements should adhere to the concept of "least privilege," include only those privileges needed for each employee to perform their duties, and be submitted to the Applications Development office in a formal work request.

> ***Management's Response:*** The IRS agreed with this recommendation. A role-based access control scheme is being developed. Once this corrective action is completed, a formal work request will be submitted to the MITS organization to implement the new access levels.

Recommendation 4: The Associate Chief Information Officer, Applications Development, should 1) create and implement a role-based access control scheme for the AIS based on the documented user requirements defined by the Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, SB/SE Division, and 2) remove the User Administrator privilege from the Developer privilege level.

> ***Management's Response:*** The IRS agreed with this recommendation. The Collection Policy office will submit a work request with documented user requirements by November 15, 2011, and the Applications Development office has removed the User Administrator privilege from the Developer privilege level.

The Online 5081 System Is Not Used to Authorize and Revoke Access to the Automated Insolvency System

To request, authorize, and revoke access to IRS computer systems, employees and managers are required to use the OL5081 system. The employee completes his or her access request on the OL5081 system, and the manager approves the request. The employees' approved access request is then routed to an employee with User Administrator privileges who adds the user to the system. If the employee needs elevated access privileges, the manager is required to document his or her approval in the special instructions section of the employees' OL5081 form.

The manager is also required to revoke an employee's access authorizations by updating the employees' OL5081 form when the employee no longer needs access. The OL5081 is then routed to a user administrator who disables the employee's access on the system.

Some managers are not using the OL5081 system to authorize and revoke their employees' access authorizations, and some employees assigned user administrator duties are not deactivating the accounts when required. Of the approximately 1,500 users with an active account on the AIS, we found:

- Fourteen employees separated from the IRS but still had an active account. For nine of these employees, the managers revoked their access approval on the OL5081 system but the account was not deactivated. The three user administrators we interviewed attributed these unauthorized accounts to oversights on their part. Although we found these 14 accounts had not been used since the employees separated, the accounts still pose an unnecessary risk because unauthorized individuals could exploit these accounts.
- Managers for 18 current employees revoked their employee's access approval on the OL5081 form but the access account was still active. Six of the seven managers we interviewed informed us the employees no longer work in the Insolvency program, do not need access to the AIS, and the user administrators should have deactivated the employees' accounts. One manager stated that one of these employees still needs AIS access but the manager did not use the OL5081 to reapprove the employee's access account.
- Sixteen of the employees' OL5081 forms contained no evidence that the employee had ever requested or been approved to access the AIS. We interviewed seven managers for seven of these employees. Five managers informed us their employee does not need AIS access and one of the five managers was not sure how the employee gained access. Two other managers stated that two of the employees need their current access to the AIS and the failure to use the OL5081 system was due to oversights by managers.

We found other instances of managers and user administrators not using the OL5081 system to revoke users' access. For 19 (18 percent) of 106 users in our sample that had an inactive account, managers did not revoke access approval in the OL5081 system. The 19 employees are still officially authorized to have access and could contact an employee with User Administrator privileges to have their account reactivated. We attribute this issue to managers bypassing the OL5081 system and using informal methods to revoke their access authorizations.

Access authorization includes more than general access to a computer system. Authorization also includes what a user can do once he or she gains access. Managers are required to approve the employees' system privileges based on the need to know and the employees' assigned duties. The manager must document his or her approval of the employee's privileges in the special instructions section of the OL5081 form and review these authorizations during the annual OL5081 recertification process. However, of the 34 AIS users in our sample, none of their managers approved their access privileges in the OL5081 form. Because the access privileges are not approved and documented in the OL5081 system, the managers cannot validate the appropriateness of employees' AIS privileges during the annual OL5081 recertification.

We interviewed 11 Insolvency program managers to discuss their responsibilities during the annual OL5081 recertification process. Ten of the 11 managers were unaware of the requirement to validate their privilege authorizations during the recertification process. The managers review employees' OL5081 forms only to determine whether the employee still needs a general level of access.

We found the same lack of control in our Fiscal Year 2009 review of access controls for the Automated Collection System.[8] In that review, we found none of the managers review the OL5081 system to determine the appropriateness of the employees' access privileges and were unaware of this requirement. In addition, we reported 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 displayed on managers' computers.

Rather than use the OL5081 system to approve users' privileges, the managers allow other employees with user administrator rights to enable system privileges that these other employees deem appropriate. For example, the Senior Technical Analyst in the Centralized Insolvency Operation office, who has user administrator privileges, assigns AIS privileges for Centralized Insolvency Operation office employees based on his knowledge of their duties and what he thinks the employees need. A manager in the Dallas Field Insolvency office, who has user administrator rights, also stated that if an employee gets promoted and needs elevated privileges, he is notified in staff meetings or is verbally informed. The manager then changes the employee's privileges in the AIS. In these instances, the manager does not document his or her approval for the privileges in the special instructions section of the OL5081 system. When managers do not properly approve and periodically check the appropriateness of their employees' access privileges, the risks of unauthorized access to taxpayers' data is increased.

In our report on the Automated Collection System, we recommended the Chief Technology Officer make a top priority the identity access provisioning and management solution to enhance the OL5081 system or replace it with a commercial off-the-shelf software product. We believe this corrective action is critical to resolve the IRS's computer security material weakness on access controls and will also improve access controls for the AIS. We will not repeat the recommendation in this report.

[8] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).

Recommendation

Recommendation 5: The Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, SB/SE Division, should issue a memorandum to managers emphasizing the requirement to use the OL5081 system to authorize, revoke, and review employees' AIS access authorizations, including employees' access privileges. The memorandum should instruct managers to verify during the annual OL5081 recertification process that their authorizations of employees' access privileges are appropriate and documented in the OL5081 system.

> **Management's Response:** The IRS agreed with this recommendation. The Directors, Collection Policy, Campus Filing and Payment Compliance, and Advisory, Insolvency, and Quality, SB/SE Division, will issue a memorandum to their managers to emphasize the requirements to use the OL5081 system to authorize, revoke, and review employees' AIS access authorization, including employees' access privileges. Managers will be instructed to verify during the annual OL5081 recertification process that their authorizations of employees' access privileges are appropriate.

Significant Automated Insolvency System Actions Taken on Bankruptcy Cases Are Not Logged and Reported in the Manager Review Screen

The AIS Manager Review screen displays most of the actions employees perform on bankruptcy cases. This screen provides audit trail information and allows managers to review employees' specific actions. However, we identified five AIS input screens that allow employees to perform significant actions on a case that are not reported in the Manager Review screen. Users could alter case information using these five input screens without detection. Managers and troubleshooters cannot determine who made a specific change to a case when employees use the following five input screens:

- The Proof of Claim screen displays and allows changes to the Proof of Claim information that the IRS filed with the bankruptcy court. This screen could be used to fictitiously indicate the IRS filed a Proof of Claim when, in fact, the IRS did not file with the court.
- The Letter screen is used to generate letters relating to bankruptcy actions and could be used by a malicious user to send incorrect or unwarranted letters to taxpayers causing confusion or undue stress on the taxpayer.
- The Payment Plan screen allows users to alter information related to taxpayer payments scheduled or received. A user could manipulate or change the data to show payments were received or never received.

- The Attorney/Trustee Information screen could be used to alter the name, address, or other personal data regarding a bankruptcy attorney or trustee. This modification would affect all cases associated with the attorney or trustee.
- The Refund screen, Request for IDRS[9] Generated Refund (IGR) (Form 5792), information could be maliciously altered to adjust information pertaining to posting a manual refund.

IRS procedures require computer systems be configured to provide audit trail tools that allow managers to hold employees accountable for their actions on computer systems. Audit trails should be enabled to monitor and log user activities such as editing and deleting records or data.

The Applications Development office informed us that the SB/SE Division's Collection function did not request the changes made to a case using the above five screens be reported in the Manager Review screen. Therefore, this audit trail capability was not configured for the AIS.

The risk of employees taking unauthorized actions without being detected, using these five screens, is further increased due to the lack of AIS database audit trail review. The MITS organization Cybersecurity office informed us that the database audit trails for the AIS are not being reviewed by the Security Auditing and Analysis System.

Recommendation

Recommendation 6: The Director, Collection Policy, SB/SE Division, should submit a work request to the Associate Chief Information Officer, Applications Development, requesting the AIS be configured to report users' changes to cases using the Proof of Claim, Letter, Payment Plan, Attorney/Trustee Information, and Refund screens. Use of these five screens should be reported in the AIS Manager Review screen to provide an audit trail of actions AIS users performed on the bankruptcy cases.

> ***Management's Response:*** The IRS agreed with this recommendation. A work request will be submitted to report users' changes to cases using the Proof of Claim, Letter, Payment Plan, Attorney/Trustee Information, and Refund screens. These changes will be captured in the AIS Manager Review screen and a Support Table Review screen to provide an audit trail.

[9] Integrated Data Retrieval System.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS has implemented access controls for the AIS to protect taxpayers' personal data and to ensure the Government's interest is protected when taxpayers file for bankruptcy. To accomplish this objective, we:

I. Determined whether key access controls are operating effectively to limit access to the AIS.

A. Determined whether controls limit access to only authorized users performing assigned duties. We determined whether users were authorized to have an access account and whether the users were authorized to have their system privileges.

1. Obtained a download of the user account control list for the AIS as of May 8, 2010. We determined the access level of the employees on the AIS user account control list.

2. Determined whether users' access privileges were approved by the user's manager by reviewing the Online 5081 (OL5081) for a judgmental sample of 34 different users. A judgmental sample was used because we wanted to determine whether a control weakness existed and we believed this sample size was sufficient to make that evaluation. Also, we did not intend to project the sample results to the population. These users worked in the Dallas, Texas, and Oakland and San Jose, California, Insolvency offices; Centralized Insolvency Operation office in the Philadelphia, Pennsylvania, Campus; and applications developers in various offices around the Nation. There were a total of 534 users in these offices. We also reviewed the OL5081 to determine whether the managers approved (recertified) the access privileges within the last 12 months and whether the users' privileges were reviewed annually by the users' managers.

3. For users without an OL5081 record and users with potentially excessive or unauthorized privileges, interviewed the users' managers to determine reasons for the specific privileges.

4. Determined whether users' roles and responsibilities were aligned with their access privileges on the AIS according to the concept of "least privilege."

5. Interviewed managers in the Centralized Insolvency Operation office and in the Field Insolvency offices to identify employees that have separated within the last 12 months.

6. Interviewed Applications Development office personnel to determine whether users' access levels on the AIS can be altered to better align with users' roles.

B. Determined whether the logins and passwords of inactive users are inactivated on the AIS. The AIS system administrator informed us that users' accounts cannot be deleted from the system if the user worked on a case maintained in the system. Instead, the users are deactivated and their login and password are deleted. We selected 106 of the 967 inactive users – the 6 employees that separated from the Texas Insolvency offices and Oakland/San Jose Insolvency offices during the 12 months prior to our audit, and the 73 Centralized Insolvency Operation office employees and 27 other users randomly selected from the AIS inactive list. We randomly picked these 100 users (73 + 27) to ensure each user had an equal chance of being selected. We also compared the AIS active users (1,526 users) from the AIS user account control list to the OL5081 system to determine whether active users were properly authorized using the OL5081 system.

C. Determined whether duties were adequately separated to limit conflicts of interest among key personnel.

D. Determined whether the system automatically locks out a user after three unsuccessful logon attempts.

E. Determined whether AIS passwords comply with IRS password complexity requirements.

F. Determined whether the AIS displays the required banner to warn unauthorized individuals that the system and its information are for authorized users only.

G. Determined whether access controls for users directly accessing the Oracle 10g database are adequate and access privileges are aligned with assigned roles and responsibilities. Reviewed user profiles, accounts, roles, and privileges.

II. Evaluated the case controls that the Centralized Insolvency Operation office implemented to process ENS records received from United States Bankruptcy Courts.

A. Determined whether managers review employees' ENS deletion actions and document their approval.

1. Requested the Audit Delete Reports for the months of June, August, October, and December 2009 and February 2010 and determined whether the appropriate managers signed and dated the reports to document their review and approval.

2. Interviewed managers to determine if cases were deleted for reasons other than duplication and whether they found any improper notice deletions or other case processing problems since the new Audit Delete Report procedure was implemented.

3. Selected a statistical random sample of deleted notices from the Audit Delete Reports and determined whether the bankruptcy notices were improperly deleted by IRS employees. We selected three Audit Delete reports that were generated during February 2010. The 3 reports listed a total of 910 deleted ENS bankruptcy notices. Our sample of 30 was based on a 5 percent precision rate, 2 percent expected error rate, and a 95 percent confidence level. We expanded our sample to include the Audit Delete Reports for June, August, October, and December 2009 to cover the 9-month period prior to our audit. A total of 7,234 ENS notice deletions were listed on these Audit Delete reports. Our second sample of 66 notices was based on a 4 percent precision rate, 2 percent expected error rate, and a 98 percent confidence level. Combined with the first sample, we tested a total 96 deleted notices.

B. Determined whether controls can be improved to prohibit unauthorized deletion of ENS bankruptcy notices by interviewing AIS Applications Development office officials and evaluating the feasibility of limiting the notice deletion privilege to the lead technicians in the Centralized Insolvency Operation office's Automated Processing Control function.

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: access controls for the AIS and case controls that the Centralized Insolvency Operation office implemented to process ENS records received from United States Bankruptcy Courts.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
W. Allen Gray, Audit Manager
Cari Fogle, Lead Auditor
Midori Ohno, Senior Auditor
Jennifer Clewis, Auditor
Frank O’Connor, Auditor
Monique Queen, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Director, Advisory, Insolvency, and Quality, Small Business/Self-Employed Division SE:S:C:AIQ
Director, Campus Filing and Payment Compliance, Small Business/Self-Employed Division SE:S:CCS:FPC
Director, Collection Policy, Small Business/Self-Employed Division SE:S C:CP
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
- Chief, Office of Appeals AP
- Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Excessive Privileges

The inadequate role-based access control scheme that the IRS developed for the AIS caused managers to inadvertently grant unneeded, excessive privileges to users. The following six examples are in addition to the four examples provided in the body of the report beginning on page 9.

Job Function	Assigned Duties/Access Level and Privileges Granted	Excessive Privileges
Planning and Analysis Quality Analyst, Campus Compliance Services	Review case work done by employees. (Access Level 2) View the Manager Review screen to identify actions taken by employees. (Manager privileges)	Update and delete case information, Case Assignment Guide, bulk processes, and delete ENS notices. Manager privileges allow user to change attorney/trustee data and employee data, perform bulk case assignments, and view Manager reports.
Field Insolvency Bankruptcy Specialist	Update bankruptcy cases and file the Proof of Claim. (Access Level 2)	Delete ENS notices.
Field Insolvency Secretary	Query AIS cases regarding requests from attorneys and taxpayers and perform bulk printing, such as printing taxpayer notices and letters. (Access Level 2) Some secretaries print Manager reports. (Manager privileges)	Change and delete case information, delete ENS notices, Case Assignment Guide, and the Payments screen. Manager privileges allow user to change attorney/trustee data and employee data, perform bulk case assignments, and view the Manager Review screen.

Job Function	Assigned Duties/Access Level and Privileges Granted	Excessive Privileges
Non-Insolvency User	Need read-only access to view case status, and sign off on case history. (Access Level 1, 2, or 3)	Update and delete case information, view and generate reports, assign or reassign cases to employees, and perform bulk processes. Users with Access Level 1 or 2 can delete ENS notices.
Application Developer	Diagnose problems related to the interfaces between the AIS and other systems. (Developer privileges)	User Administrator privileges allow user to add users, create passwords, and assign privileges.
Troubleshooter	View case information to help users with their AIS problems. (Access Level 1, Manager, Analyst, and User Administrator privileges)	Update and delete case information and ENS notices, and perform bulk processes. Manager privileges allow user to perform bulk case assignments. User Administrator privileges allow user to create new users, create passwords, and assign privileges.

Appendix V

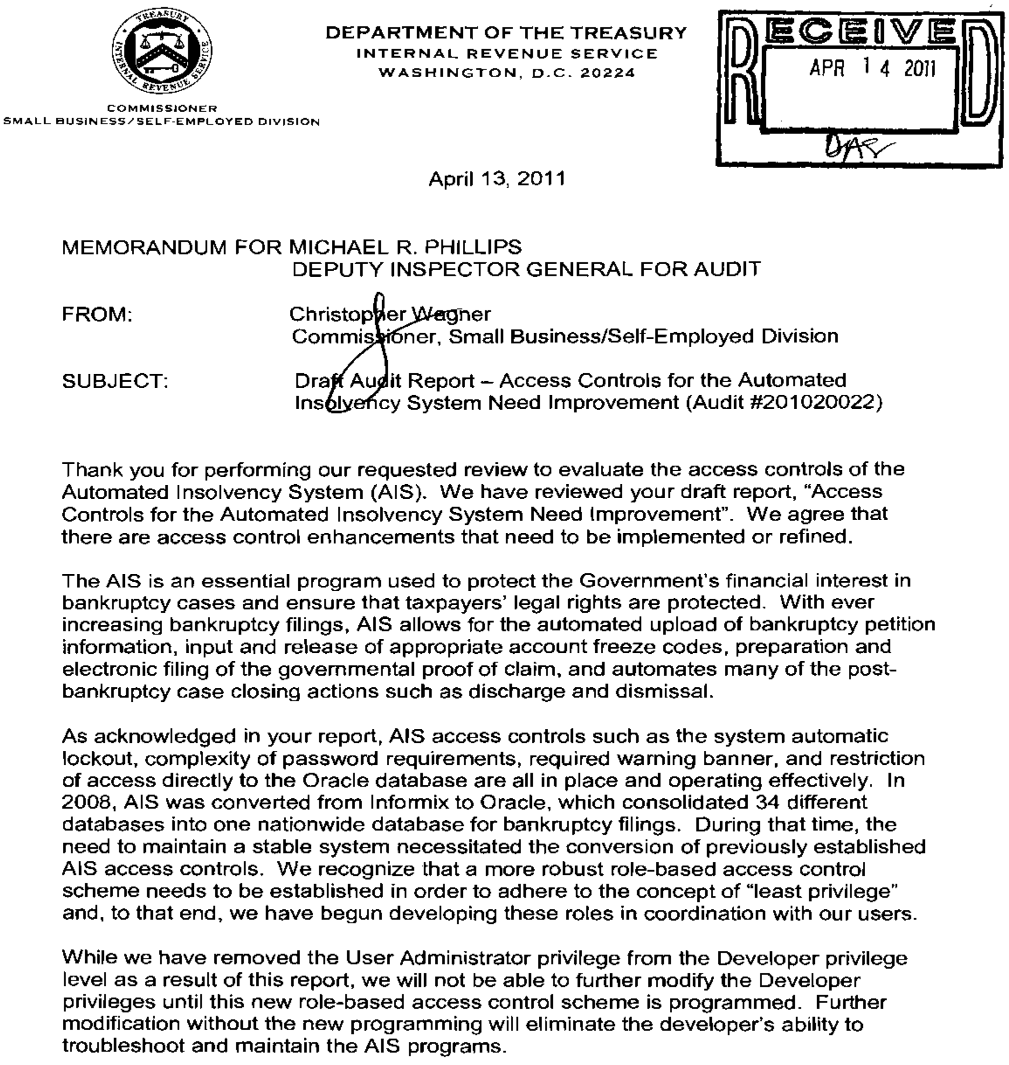
Glossary of Terms

Term	Definition
Automated Collection System	A telephone contact system through which telephone assistors collect unpaid taxes and secure tax returns from delinquent taxpayers who have not complied with previous notices.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Computing Center	IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
Concept of "least privilege"	A key internal control concept and IRS requirement. The intent to minimize employees' system access privileges to the minimum needed to perform assigned duties.
Configuration Control	The management of security features and assurances through control of changes made to hardware and software throughout the life cycle of a computer system.
Integrated Data Retrieval System	A major IRS application consisting of databases and operating systems that support IRS employees working active tax cases within each business function across the IRS. This system allows employees to post transaction updates to the IRS master files.
Informix	Informix is a relational database management system developed by the International Business Machines Corporation and is used for online transaction processing.

Term	Definition
Online 5081 System	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 Information System User Registration/Change Request (Form 5081) with an automated, standard process. It provides automated submission, approval, recertification, and filing of the Form 5081 on an enterprise-wide basis.
Oracle	The Oracle Database is a relational database management system produced by the Oracle Corporation.
Proof of Claim	An official form filed with a Bankruptcy court describing the reason a debtor owes creditor money, which typically sets forth the amount of money owed.
Role-Based Access Control	A security approach to restricting employees' access to computer systems. System roles are created for an organization's various job functions. The minimum privileges needed to perform the job functions are assigned to the roles. The role is then assigned to a system user.
Security Auditing and Analysis System	The Security Audit and Analysis System implements a data warehousing solution to provide online analytical processing of audit trail data.
Separation of Duties	A key internal control concept. The objective is for management to assign duties and implement checks and balances upon the activities of employees to prevent errors and fraud. For example, organizations separate the duties of receiving customers' checks and approving account write-offs, and depositing cash and reconciling bank statements.
Transmittal	The purpose of a Transmittal is to either document changes to an 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.

Appendix VI

Management's Response to the Draft Report



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

COMMISSIONER
SMALL BUSINESS/SELF-EMPLOYED DIVISION

April 13, 2011

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Christopher Wagner
Commissioner, Small Business/Self-Employed Division

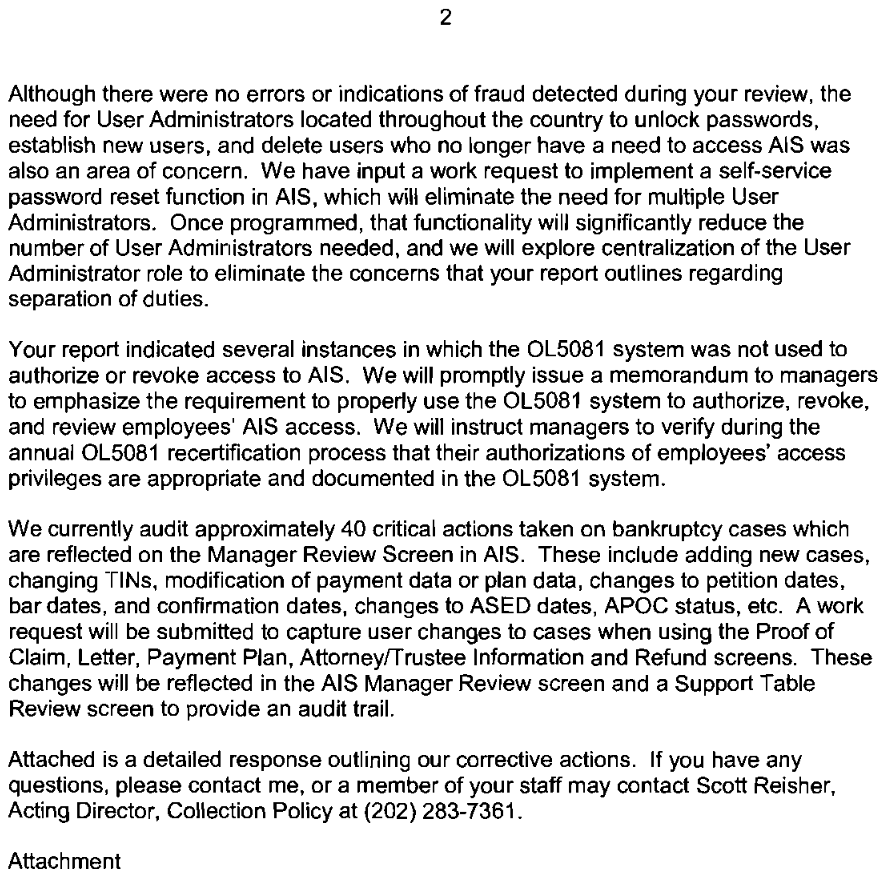
SUBJECT: Draft Audit Report – Access Controls for the Automated Insolvency System Need Improvement (Audit #201020022)

Thank you for performing our requested review to evaluate the access controls of the Automated Insolvency System (AIS). We have reviewed your draft report, "Access Controls for the Automated Insolvency System Need Improvement". We agree that there are access control enhancements that need to be implemented or refined.

The AIS is an essential program used to protect the Government's financial interest in bankruptcy cases and ensure that taxpayers' legal rights are protected. With ever increasing bankruptcy filings, AIS allows for the automated upload of bankruptcy petition information, input and release of appropriate account freeze codes, preparation and electronic filing of the governmental proof of claim, and automates many of the post-bankruptcy case closing actions such as discharge and dismissal.

As acknowledged in your report, AIS access controls such as the system automatic lockout, complexity of password requirements, required warning banner, and restriction of access directly to the Oracle database are all in place and operating effectively. In 2008, AIS was converted from Informix to Oracle, which consolidated 34 different databases into one nationwide database for bankruptcy filings. During that time, the need to maintain a stable system necessitated the conversion of previously established AIS access controls. We recognize that a more robust role-based access control scheme needs to be established in order to adhere to the concept of "least privilege" and, to that end, we have begun developing these roles in coordination with our users.

While we have removed the User Administrator privilege from the Developer privilege level as a result of this report, we will not be able to further modify the Developer privileges until this new role-based access control scheme is programmed. Further modification without the new programming will eliminate the developer's ability to troubleshoot and maintain the AIS programs.



2

Although there were no errors or indications of fraud detected during your review, the need for User Administrators located throughout the country to unlock passwords, establish new users, and delete users who no longer have a need to access AIS was also an area of concern. We have input a work request to implement a self-service password reset function in AIS, which will eliminate the need for multiple User Administrators. Once programmed, that functionality will significantly reduce the number of User Administrators needed, and we will explore centralization of the User Administrator role to eliminate the concerns that your report outlines regarding separation of duties.

Your report indicated several instances in which the OL5081 system was not used to authorize or revoke access to AIS. We will promptly issue a memorandum to managers to emphasize the requirement to properly use the OL5081 system to authorize, revoke, and review employees' AIS access. We will instruct managers to verify during the annual OL5081 recertification process that their authorizations of employees' access privileges are appropriate and documented in the OL5081 system.

We currently audit approximately 40 critical actions taken on bankruptcy cases which are reflected on the Manager Review Screen in AIS. These include adding new cases, changing TINs, modification of payment data or plan data, changes to petition dates, bar dates, and confirmation dates, changes to ASED dates, APOC status, etc. A work request will be submitted to capture user changes to cases when using the Proof of Claim, Letter, Payment Plan, Attorney/Trustee Information and Refund screens. These changes will be reflected in the AIS Manager Review screen and a Support Table Review screen to provide an audit trail.

Attached is a detailed response outlining our corrective actions. If you have any questions, please contact me, or a member of your staff may contact Scott Reisher, Acting Director, Collection Policy at (202) 283-7361.

Attachment

Attachment

RECOMMENDATION 1:
The Directors of Collection Policy, Filing and Payment Compliance and Advisory, Insolvency, and Quality should 1) identify incompatible duties and implement policies to segregate those duties, 2) issue a memorandum to Insolvency program managers requiring them to adhere to the new policy when assigning duties and approving AIS access privileges, and 3) designate a limited number of employees to perform the User Administrator duties. These employees should have no more capability than necessary to establish a user on the AIS.

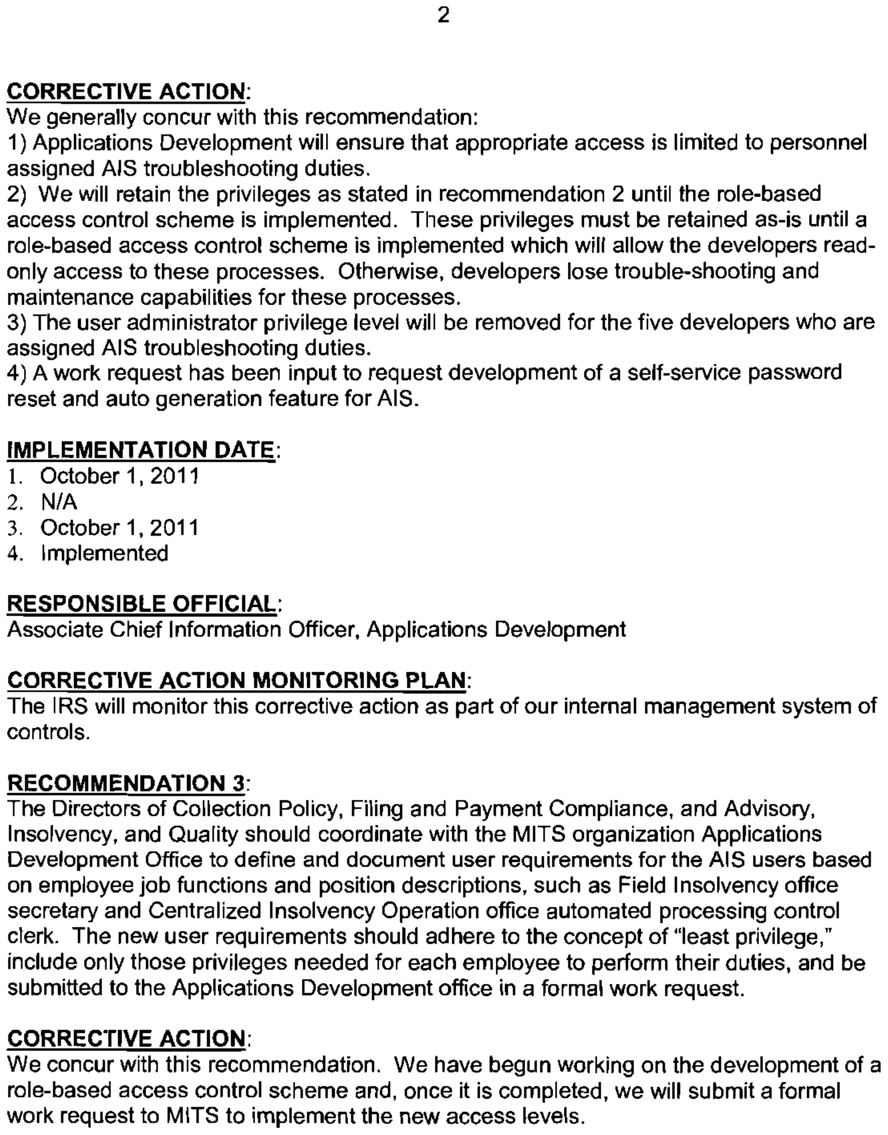
CORRECTIVE ACTION:
We concur with this recommendation. A role-based access control system is currently being developed which will define the roles of users and designate specific access privileges to their defined AIS profiles. Once this process is established, a memorandum will be issued to all managers requiring them to adhere to the new policy regarding segregation of duties. Policy and MITS are working on reprogramming of AIS to allow users to reset their passwords as opposed to the current process in which a User Administrator must reset passwords. This would dramatically reduce the number of User Administrators needed.

IMPLEMENTATION DATE:
January 15, 2012

RESPONSIBLE OFFICIAL(S):
Directors of Collection Policy, Filing and Payment Compliance and Advisory, Insolvency, and Quality

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2:
The Associate Chief Information Officer, Applications Development, should 1) remove the access account of the three application developers who are not assigned AIS troubleshooting duties, 2) remove the Access Level 1 and Manager privileges for the eight developers who are assigned troubleshooting duties and ensure they have only the Developer privileges and read-only access, 3) remove the User Administrator privilege level for the five developers who are assigned troubleshooting duties, and 4) develop a software product to systemically create and assign passwords for new AIS users.



2

CORRECTIVE ACTION:
We generally concur with this recommendation:
1) Applications Development will ensure that appropriate access is limited to personnel assigned AIS troubleshooting duties.
2) We will retain the privileges as stated in recommendation 2 until the role-based access control scheme is implemented. These privileges must be retained as-is until a role-based access control scheme is implemented which will allow the developers read-only access to these processes. Otherwise, developers lose trouble-shooting and maintenance capabilities for these processes.
3) The user administrator privilege level will be removed for the five developers who are assigned AIS troubleshooting duties.
4) A work request has been input to request development of a self-service password reset and auto generation feature for AIS.

IMPLEMENTATION DATE:
1. October 1, 2011
2. N/A
3. October 1, 2011
4. Implemented

RESPONSIBLE OFFICIAL:
Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3:
The Directors of Collection Policy, Filing and Payment Compliance, and Advisory, Insolvency, and Quality should coordinate with the MITS organization Applications Development Office to define and document user requirements for the AIS users based on employee job functions and position descriptions, such as Field Insolvency office secretary and Centralized Insolvency Operation office automated processing control clerk. The new user requirements should adhere to the concept of "least privilege," include only those privileges needed for each employee to perform their duties, and be submitted to the Applications Development office in a formal work request.

CORRECTIVE ACTION:
We concur with this recommendation. We have begun working on the development of a role-based access control scheme and, once it is completed, we will submit a formal work request to MITS to implement the new access levels.

IMPLEMENTATION DATE:
November 15, 2011

RESPONSIBLE OFFICIAL(S):
Director, Collection Policy, Director, Filing and Payment Compliance, and Director, Advisory, Insolvency and Quality

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.

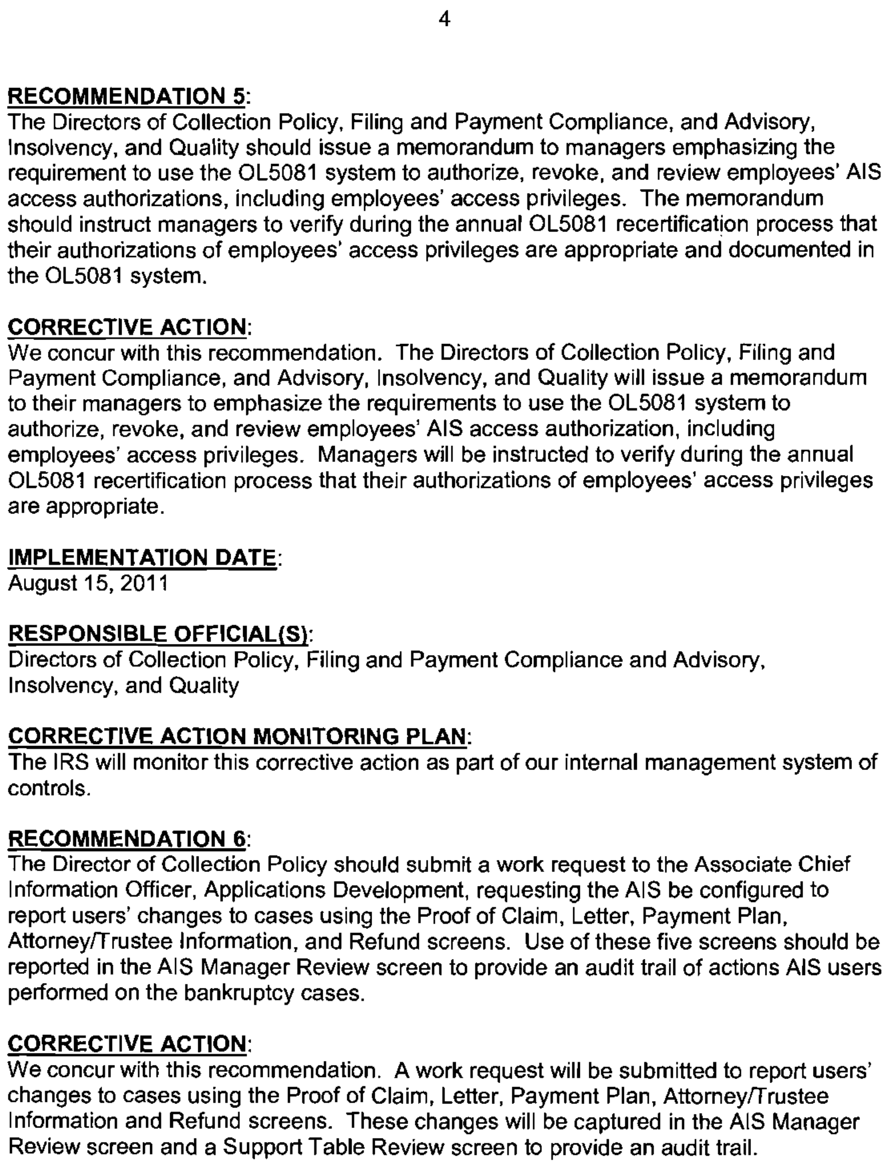
RECOMMENDATION 4:
The Associate Chief Information Officer, Applications Development, should 1) create and implement a role-based access control scheme for the AIS based on the documented user requirements defined by the Directors, Collection Policy, Filing and Payment Compliance, and Advisory, Insolvency, and Quality, and 2) remove the User Administrator privilege from the Developer privilege level.

CORRECTIVE ACTION:
We concur with this recommendation:
1) SBSE Collection will submit a work request with documented user requirements by November 15, 2011.
2) Applications Development has removed the User Administrator privilege from the Developer level privilege.

IMPLEMENTATION DATE:
1) November 15, 2011
2) Implemented

RESPONSIBLE OFFICIAL:
Director, Collection Policy, Director, Filing and Payment Compliance, and Director, Advisory, Insolvency and Quality

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.



4

RECOMMENDATION 5:
The Directors of Collection Policy, Filing and Payment Compliance, and Advisory, Insolvency, and Quality should issue a memorandum to managers emphasizing the requirement to use the OL5081 system to authorize, revoke, and review employees' AIS access authorizations, including employees' access privileges. The memorandum should instruct managers to verify during the annual OL5081 recertification process that their authorizations of employees' access privileges are appropriate and documented in the OL5081 system.

CORRECTIVE ACTION:
We concur with this recommendation. The Directors of Collection Policy, Filing and Payment Compliance, and Advisory, Insolvency, and Quality will issue a memorandum to their managers to emphasize the requirements to use the OL5081 system to authorize, revoke, and review employees' AIS access authorization, including employees' access privileges. Managers will be instructed to verify during the annual OL5081 recertification process that their authorizations of employees' access privileges are appropriate.

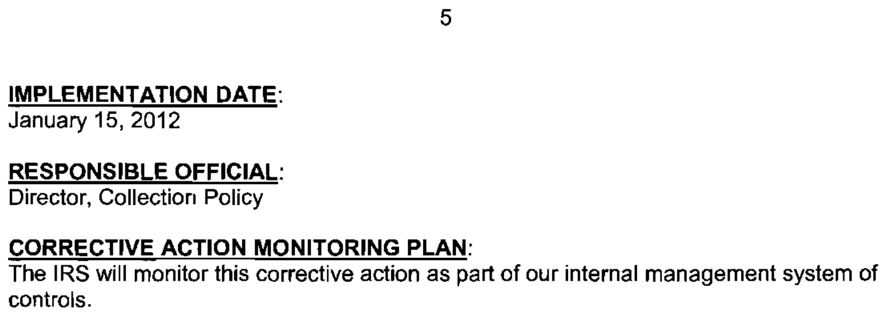
IMPLEMENTATION DATE:
August 15, 2011

RESPONSIBLE OFFICIAL(S):
Directors of Collection Policy, Filing and Payment Compliance and Advisory, Insolvency, and Quality

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 6:
The Director of Collection Policy should submit a work request to the Associate Chief Information Officer, Applications Development, requesting the AIS be configured to report users' changes to cases using the Proof of Claim, Letter, Payment Plan, Attorney/Trustee Information, and Refund screens. Use of these five screens should be reported in the AIS Manager Review screen to provide an audit trail of actions AIS users performed on the bankruptcy cases.

CORRECTIVE ACTION:
We concur with this recommendation. A work request will be submitted to report users' changes to cases using the Proof of Claim, Letter, Payment Plan, Attorney/Trustee Information and Refund screens. These changes will be captured in the AIS Manager Review screen and a Support Table Review screen to provide an audit trail.



IMPLEMENTATION DATE:
January 15, 2012

RESPONSIBLE OFFICIAL:
Director, Collection Policy

CORRECTIVE ACTION MONITORING PLAN:
The IRS will monitor this corrective action as part of our internal management system of controls.