



*Effectiveness of Access Controls Over  
System Administrator User Accounts  
Can Be Improved*

**September 19, 2007**

**Reference Number: 2007-20-161**

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.

---

*Phone Number* | 202-927-7037

*Email Address* | [Bonnie.Heald@tigta.treas.gov](mailto:Bonnie.Heald@tigta.treas.gov)

*Web Site* | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

September 19, 2007

**MEMORANDUM FOR CHIEF INFORMATION OFFICER**

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

**SUBJECT:** Final Audit Report – Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved (Audit # 200620032)

This report presents the results of our review of the effectiveness of access controls over system administrator user accounts on Internal Revenue Service (IRS) computers. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2006 Annual Audit Plan and was part of the Information Systems Programs unit's statutory requirements to annually review the adequacy and security of IRS technology.

*Impact on the Taxpayer*

To perform their job responsibilities, system administrators must be given total control over computer systems. Due to the sensitive nature of the system administrator position, the IRS must have proper controls in place to ensure only appropriate employees have administrator rights and privileges, administrator user accounts are reviewed annually for continued business need, their user accounts are protected with strong passwords, and their actions on computer systems are monitored for questionable activities. However, administrator user accounts were not always authorized and maintained properly, and administrator activities were not consistently reviewed and documented. Weak controls over user accounts could allow unauthorized individuals to gain access to these accounts, which could lead to unauthorized disclosure of taxpayer data and disruptions of service affecting work productivity and revenue collection.

*Synopsis*

The IRS has over 260 computer system applications to process tax records for 130 million taxpayers and to support and assist its employees in administering the nation's tax system. To properly carry out their duties and protect data in systems considered sensitive,



## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

system administrators are normally granted full control over computer systems, in effect providing them unrestricted access and authority over the systems.

While the IRS has established appropriate procedures for authorizing and maintaining administrator user accounts as well as procedures to review their user account activities for improprieties, we identified the following problems. These weaknesses occurred because managers and system administrators did not adhere to procedures.

First, the IRS is not approving and maintaining proper documentation for establishing administrator user accounts. We could not find authorization and approval documentation for 31 (5 percent) of 607 user accounts for the 5 applications we reviewed. IRS managers informed us that paper authorization forms were never entered into the IRS computer system used to track user accounts for all IRS applications and the paper forms have since been destroyed. Because no proof exists that these active user accounts were authorized, we have no assurance these accounts are legitimate, which increases the IRS' vulnerability to unauthorized access and fraudulent activities.

Second, the IRS had unnecessary administrator user accounts. Seventy-nine (13 percent) of 607 active user accounts were not needed because the employees no longer had a business need to administer their respective computer systems. To address account review requirements, the IRS created automated computer programs (scripts) to identify user accounts with inactivity and to disable and remove those accounts meeting this criterion. Because managers and administrators were relying on these scripts, they were not reviewing accounts or reports on inactivity to identify potential accounts that were no longer needed. However, we identified programming errors in the scripts that caused them to not properly identify all accounts with inactivity.

Third, weak passwords on user accounts existed on all five applications we reviewed because systemic password mechanisms did not adhere to required IRS password standards. The applications were running on an outdated operating system that would allow for the use of passwords that met standards but would not reject those passwords that did not meet standards. As a result, managers and administrators may not be voluntarily complying with password standards.

Finally, audit trails<sup>1</sup> are not being reviewed for four of the five applications we reviewed. While the IRS was capturing every key stroke from administrator user accounts and sending the data offsite for backup purposes for three of the four applications, it was not conducting regular reviews of the audit trails. Capacity and performance problems have plagued the IRS' implementation of an audit trail solution for its Unix-based servers. As a result, the IRS allowed

---

<sup>1</sup> An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.



## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

the user license to expire in September 2006, and the audit trail solution product is no longer being used.

The existence of active administrator user accounts with weak passwords for employees who no longer have a business need poses an unnecessary risk for unauthorized disclosure of taxpayer data and disruption of computer operations. Because of the trust relationship among computers on the network, inadequate access controls over these user accounts could allow hackers and disgruntled employees to have access to other computers on the network. In addition, when audit trails are not being reviewed, the IRS may not be detecting improper administrator activities on computer system applications.

### *Recommendations*

We recommended the Chief Information Officer ensure managers identify system administrator user accounts on all applications that do not have proper authorization documentation, assess whether the accounts are still needed, and establish appropriate authorization documentation for those accounts; test the automated computer programs (scripts) used to deactivate and/or delete administrator user accounts with periods of inactivity; and reinforce the need for managers of system administrators to be cognizant of the applications their employees can access and limit those access rights to only those applications needed to carry out their responsibilities. The Chief Information Officer should also ensure the deployment of the host-based intrusion detection software continues to ensure audit trail reviews over administrator user accounts on Tier 2 Unix-based servers.

### *Response*

The Chief Information Officer agreed with our recommendations. A process will be implemented to review system administrator user accounts on all systems at least annually to ensure only those system administrator user accounts with a continued business need exist on IRS systems, the feature of the operating systems will be implemented to identify and delete all system administrator user accounts with no activity for 45 days, and a notice will be sent to all managers of system administrators to reinforce the need to be aware of the applications their system administrators can access and to limit those access rights to only those applications needed to carry out their responsibilities. In addition, Host-based Intrusion Detection Sensor agents will be deployed on Tier 2 Unix-based servers. Management's complete response to the draft report is included as Appendix V.

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 Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.



---

*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

*Table of Contents*

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

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

    System Administrator User Accounts Were Not Always  
    Authorized and Maintained Properly .....Page 3

Recommendations 1 through 3:.....Page 7

    Audit Trails Are Not Consistently Reviewed and Documented .....Page 8

Recommendation 4:.....Page 9

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 10

    Appendix II – Major Contributors to This Report .....Page 12

    Appendix III – Report Distribution List .....Page 13

    Appendix IV – Description of Internal Revenue Service  
    Applications Selected for Review .....Page 14

    Appendix V – Management’s Response to the Draft Report .....Page 15



*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

*Abbreviations*

AIMS	Audit Information Management System
ALS	Automated Lien System
ASFR	Automated Substitute for Return System
ELS	Electronic Levy System
eTrust®	eTrust® Access Control and Audit
ExFIRS	Excise Files Information Retrieval System
IRS	Internal Revenue Service
OL5081	On-Line Form 5081



---

## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

### *Background*

The Internal Revenue Service (IRS) has over 260 computer system applications to process tax records for 130 million taxpayers and to support and assist its employees in administering the nation's tax system. The data in these systems are considered sensitive and require protection from unauthorized use, modification, disclosure, and destruction. The importance of protecting these data was illustrated with passage of the Taxpayer Browsing Protection Act of 1997.<sup>1</sup> This Act makes the willful unauthorized access and inspection of taxpayer records a crime; it applies to IRS employees to ensure they do not abuse their authority on accessing taxpayer records.

To ensure computer systems are operating as intended and are secure, the IRS has designated system administrators (also referred to as administrators) as the employees responsible for maintaining computer systems. Maintenance duties include monitoring system performance, responding to system outages or problems, adjusting settings and configurations for security and operational purposes, installing system and security patches, and installing peripheral devices. To properly carry out these duties, administrators must be given total control over computer systems, in effect providing them unrestricted access and authority over the systems. Due to the sensitive nature of having such capabilities, the IRS must have proper controls in place to ensure only appropriate employees have administrator rights and privileges and these employees do not abuse their authority.

***System administrators are normally granted full control over computer systems, in effect providing them unrestricted access and authority over the systems.***

We evaluated the IRS' controls over administrator accounts on the following five computer applications (systems) we judgmentally selected for our review. Appendix IV provides a description of these systems.

- Audit Information Management System (AIMS).
- Automated Lien System (ALS).
- Automated Substitute for Return (ASFR) System.
- Electronic Levy System (ELS).
- Excise Files Information Retrieval System (ExFIRS).

This review was performed in the Modernization and Information Technology Services organization and the former Mission Assurance and Security Services organization in

---

<sup>1</sup> 26 U.S.C.A. Sections 7213, 7213A, 7431 (West Supp. 2003).



*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

New Carrollton, Maryland, and the Enterprise Computing Centers<sup>2</sup> in Detroit, Michigan, and Memphis, Tennessee, during the period January 2007 through May 2007. The audit was conducted in accordance with *Government Auditing Standards*. 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> IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.



---

## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

### *Results of Review*

#### **System Administrator User Accounts Were Not Always Authorized and Maintained Properly**

The IRS has established appropriate procedures for authorizing and maintaining administrator user accounts. The process to establish a user account starts when an employee completes an Information System User Registration/Change Request [On-Line Form 5081(OL5081)]<sup>3</sup> to gain administrator access to a particular computer system or application. When the request contains all necessary information, the OL5081 system sends an email message to the employee's manager, who will need to access the OL5081 system to approve the request. Once the request has been approved, the OL5081 system generates an email to an existing administrator over the particular computer system or application and this designated administrator will create a new user account for the employee. The employee is then notified that his or her user account is active and ready for access. Annually, the OL5081 system sends an email to both the manager and employee to recertify that the administrator's system accesses are still appropriate and necessary. To delete an employee who no longer has a need to access a system, the manager initiates the user account removal process on the OL5081 system. An email is then sent to another administrator to remove the user account.

Although the OL5081 system automates the process for creating, maintaining, and deleting user accounts, certain actions continue to require human initiation and intervention. For example, managers must ensure employees need access to a system before granting access and promptly notify the administrators to remove employees from the system when access is no longer necessary. Managers are also required to annually review the appropriateness of their employees' access privileges. In addition, designated administrators are responsible for adding and removing system user accounts, including other administrator user accounts, when authorized; maintaining an up-to-date list of authorized users; and annually generating a list of current system users and their access profiles to provide to the appropriate managers for review.

Managers and system administrators did not adhere to system review procedures. As a result, our review of the five applications determined:

---

<sup>3</sup> The IRS uses the Information System User Registration/Change Request (Form 5081) to request and authorize user accounts for all systems. The OL5081 is an automated version of this Form. The OL5081 system was named after the Form 5081; it automates some of the manual processes and provides a centralized system for all system access authorizations.



---

## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

- Documentation for authorizations of user accounts could not be located.
- Active user accounts existed for employees who no longer had a business need.
- Password complexity did not meet IRS standards.

### **Documentation for authorization of system administrator user accounts could not be located**

Generally, the IRS is approving and maintaining proper documentation for establishing user accounts. However, we could not find authorization and approval documentation for 31 (5 percent) of 607 user accounts for the 5 applications reviewed. IRS managers informed us that paper Forms 5081 for those user accounts were never converted to the OL5081 system when it was first established and the paper Forms 5081 have since been destroyed. Because no proof exists that these active user accounts were authorized, we have no assurance these accounts are legitimate, which increases the IRS' vulnerability to unauthorized access and fraudulent activities. While 5 percent may seem low and acceptable, the capabilities of these user accounts magnify the risk because they have unlimited control over computers.

We followed up with administrator managers to determine whether these user accounts were still needed; the managers took action to establish OL5081 records for 15 of the 31 user accounts and deleted the remaining 16 user accounts because they were no longer needed. Because of the lack of readily available authorization documentation, we could not determine whether these 16 user accounts were ever truly authorized. We did determine that none of the 16 user accounts were ever accessed.

### **Active system administrator user accounts existed for employees who no longer had a business need**

In the 5 applications we reviewed, 79 (13 percent) of 607 active user accounts were not needed because the administrators no longer had a business need to administer their respective computer systems, according to their managers. These 79 user accounts included the aforementioned 16 user accounts for which we were unable to locate authorization documentation.

In addition, for 72 of the 79 user accounts, the administrators either never logged onto the system or had not logged onto the system in the past 90 calendar days. Figure 1 presents these numbers by the systems reviewed.



*Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

**Figure 1: Active System Administrator User Accounts Without a Business Need**

System Name	Number of Total User Accounts	Number of User Accounts Identified With No Business Need	Number of User Accounts Identified With No Business Need and Never Logged On	Number of User Accounts Identified With No Business Need and Not Logged On in the Past 90 Calendar Days	Number of User Accounts Identified With No Business Need and Logged On in the Past 90 Calendar Days
AIMS	137	0	0	0	0
ALS	89	2	0	2	0
ASFR	99	4	0	4	0
ELS	92	7	0	5	2
ExFIRS	190	66	29	32	5
Totals	607	79	29	43	7

Source: Treasury Inspector General for Tax Administration analysis.

Further analysis revealed 6 of the 79 user accounts belonged to IRS contractors who no longer work for the IRS. The contractors were first granted system access in November 2003, but system records show the contractors had never logged onto the system. The user accounts remained active and with the initial password assigned when the accounts were first established.

The IRS requires a user account (1) to be disabled if the user has not used the system in the past 45 calendar days and (2) to be removed if the user has not used the system in the past 90 calendar days. To address these requirements, the IRS created automated computer programs (scripts) to identify user accounts with inactivity and to disable and remove those accounts meeting these criteria. Because managers and administrators were relying on these scripts, they were not reviewing accounts or reports on inactivity to identify potential accounts that were no longer needed. However, we identified programming errors in the scripts that caused them to not properly identify those user accounts for which the administrator had never logged onto the account and for which linked user accounts<sup>4</sup> existed. As a result, inactive user accounts were not being identified and removed. Had the scripts worked properly, they would have identified 72 (91 percent) of the 79 user accounts as no longer being needed and properly disabled and removed them.

Also, administrator managers may be unaware of whether their employees continue to have a business need for system access as part of the OL5081 annual recertification process. As stated above, employees' managers are required to review the appropriateness of their employees' access privileges and to annually recertify, along with the employee, on the OL5081 system. For the user accounts reviewed, we contacted the employees' managers of record listed on the OL5081 system to confirm whether the employees continued to need access to the systems.

<sup>4</sup> These are switch-user accounts that allow system administrators to log on as a normal user and then switch user rights, when necessary, giving them root status access and full system administrative control over the system.



---

## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

These managers of record could not make that determination and deferred to the managers of the systems being reviewed. This situation illustrates the confusion over who may be in the best position to serve as the certifying official.

The existence of active user accounts with system administrative rights for employees who no longer have a business need poses an unnecessary risk for unauthorized access and disclosure of taxpayer data. These types of accounts could allow hackers and disgruntled employees to have unabated access to the computer and its data. Because computer systems within a network have a trust relationship among other computers on the network, the risk extends to other computer systems as well. We attempted to use system records to determine whether any of the 79 user accounts had been potentially misused. However, the records were not maintained in a format that could be used to identify improper activity.

### **Password complexity did not meet standards**

Weak passwords existed on system administrator user accounts on all five applications we reviewed. On one application, the passwords were not restricted to an eight-character minimum. All five applications did not enforce the following password requirements:

- Passwords must contain alpha and numeric characters and be case sensitive.
- Password history must capture the last 24 passwords used to prevent reuse.
- Passwords for user accounts must change at least every 60 calendar days.

The applications were running on an outdated operating system that would allow for the use of passwords that met standards but would not reject those passwords that did not meet standards. As a result, managers and administrators may not be voluntarily complying with password standards. This systemic weakness could allow a simple password such as “password” to be used. Due to the sensitivity of passwords, we did not attempt to reveal or obtain the actual passwords used by the administrators.

Local management informed us that the IRS is in the process of upgrading its servers, which will be capable of enforcing the password requirements. We confirmed that one of the applications we reviewed was upgraded, as of June 2007, and all password requirements were being enforced. However, we did not receive a definitive timetable for upgrading the rest of the applications. Because the IRS is taking the necessary actions to address this security weakness, we made no formal recommendations specific to this issue. However, we encourage administrator managers to emphasize the password standards and to stress the potential vulnerabilities of using weak passwords until servers have been upgraded to allow IRS password standards to be enforced.

Weak passwords over administrator user accounts leave the IRS vulnerable to hacker attacks. Disgruntled employees can employ password-hacking techniques to take over user accounts that, if successful, would give them complete access to the computer system and its resources, such as taxpayer data and password files. This scenario could lead to potential disclosure of taxpayer data.



---

*Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

## **Recommendations**

To improve access controls over system administrator user accounts, we recommend the Chief Information Officer ensure managers:

**Recommendation 1:** Identify and reconcile system administrator user accounts on all systems to the OL5081 system. For those accounts not on the OL5081 system, the system owner and the system administrator's manager should determine whether the employee continues to have a business need for access. If he or she no longer has a business need, the user account should be deleted. If he or she continues to have a business need, the manager should initiate the process of creating an OL5081 record for the user account.

**Management's Response:** The Chief Information Officer agreed with the recommendation and will implement a process to review and compare system administrator user accounts on all systems to the OL5081 system at least annually. This process will ensure system administrator user accounts with a continued business need exist on IRS systems.

**Recommendation 2:** Test the automated computer programs (scripts) used to identify and disable system administrator user accounts with 45 calendar days of inactivity, delete administrator user accounts with 90 calendar days of inactivity, and periodically validate the results to ensure the programs are working as intended.

**Management's Response:** The Chief Information Officer agreed with this recommendation and will implement the feature of the operating systems to identify and delete system administrator user accounts with 45 days of inactivity. An additional script will be added on all Unix systems to ensure system administrator user accounts will be removed after 90 days of inactivity. Quarterly, a review of systems will be completed to ensure these automated processes are working as intended.

**Recommendation 3:** Reinforce the need for system administrator managers to be cognizant of the applications their employees can access and limit those access rights to only those applications needed to carry out their responsibilities. Managers should consider long periods of inactivity when determining whether to recertify access rights on the OL5081 system.

**Management's Response:** The Chief Information Officer agreed with this recommendation and will issue to all managers of system administrators a notice to reinforce the need to be aware of the applications their system administrators can access and to limit those access rights to only those applications needed to carry out their responsibilities. The notice will also remind managers that long periods of inactivity should be considered in determining access needs when recertifying on the OL5081 system.



---

*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

### ***Audit Trails Are Not Consistently Reviewed and Documented***

Audit trails<sup>5</sup> are not being reviewed for four of the five applications. All four applications are running on Tier 2 Unix-based servers using an audit software product called eTrust<sup>®</sup> Access Control and Audit (eTrust<sup>®</sup>). For one of the four applications, the IRS is not capturing or reviewing any audit trail information. For the other three applications, the IRS is capturing every key stroke and sending it offsite for backup. However, the IRS is not generating audit trail reports and conducting regular reviews of the audit trails. A security specialist stated that audit trail analysis may occur if a specific request is made, although these requests are infrequent. Such analysis is difficult and would involve manually scrolling through the audit trail files and trying to identify specific activity. If any questionable activity is identified, the security specialist would report it to the Computer Security Incident Response Center.

We requested audit trail information for the 79 administrator user accounts that were no longer needed, to determine whether questionable activities might have occurred for those accounts. While the security specialists over the systems reviewed had initially agreed to provide us with the information, they later informed us that the process to access the information from the backup system and to convert the raw data into a useable format was very time consuming, required too much computer processing resources, and would take personnel from their normal duties to complete the task. Because of these limitations, we question the practical ability to create reviewable audit trail information when needed.

Department of the Treasury procedures require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected. These procedures also state that designated personnel must review audit trails at least weekly for systems that contain sensitive information. IRS procedures require that, at a minimum, audit trails include sufficient information to establish what events occurred, when the events occurred, and who (or what) caused them.

Due to the capacity and performance problems that have plagued the IRS' implementation of eTrust<sup>®</sup> for auditing of its Unix-based servers, the IRS has had to replace the product. At one time, the eTrust<sup>®</sup> solution was used to provide audit trail analysis but never fully delivered in its reports or analysis. For example, there were problems with the eTrust<sup>®</sup> reports. Some were simple formatting and sorting errors, but others were more significant, such as incorrect event status and reporting of erroneous events that were not requested. Also, eTrust<sup>®</sup> could collect audit logs only in text and not in the binary format necessary to run specific audit modules. Because of these problems, the IRS allowed the user license for eTrust<sup>®</sup> to expire in September 2006, and the product is no longer being used. A discussion with the Director, Information Technology Security, determined that, in late May 2007, the IRS planned to begin an enterprise

---

<sup>5</sup> An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.



---

## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

deployment of host-based intrusion detection software to monitor alerts and log files on servers for suspicious activities and to report in near real-time to the Computer Security Incident Response Center and Information Technology Security Field Specialists.

Even the best controls designed to prevent improper computer activity can be circumvented with the proper expertise. Disgruntled administrators and contractors who already have administrator access rights to a system may attempt to circumvent IRS controls to gain access to sensitive information or to vandalize computer data and processing. To help minimize these risks, routine generation and review of audit trails can assist in detecting improper activities.

### ***Recommendation***

***Recommendation 4:*** The Chief Information Officer should ensure the deployment of the host-based intrusion detection software continues to ensure audit trail reviews over system administrator user accounts on Tier 2 Unix-based servers.

***Management's Response:*** The Chief Information Officer agreed with this recommendation and will deploy the Host-based Intrusion Detection Sensor agents on Tier 2 Unix-based servers. In addition, the Cybersecurity organization, specifically Information Technology Security function field specialists, will be responsible for monitoring and reviewing event logs and alerting the Computer Security Incident Response Center of unusual or suspicious activity.



---

*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine the effectiveness of access controls over system administrator user accounts on IRS computers. To accomplish our objective, we:

- I. Determined whether system administrator user accounts had been properly approved by reviewing the OL5081 system<sup>1</sup> for all 607 administrator user accounts on 5 selected applications (systems).<sup>2</sup> From a population of 59 major applications, we judgmentally selected the 5 applications based on the risk of the application and prior Treasury Inspector General for Tax Administration audit coverage. Specifically, we:
  - A. Identified any other method (besides the OL5081 system) used for authorizing and approving the creation of administrator user accounts on systems.
  - B. Compared each user on each application's list of administrators to the OL5081 system records. For any accounts not on the OL5081 system, we determined whether paper records existed.
  - C. Reviewed Forms 5081 for proper approvals.
  - D. Where appropriate, consulted with administrators and managers to determine why no Form 5081 existed, why the Form 5081 did not contain proper approval, how long the administrator had access to the computer system without authorization, and whether any of these conditions could have been resolved by the proposals from the OL5081 system projects that are currently in process.
- II. Determined whether unnecessary system administrator user accounts, such as accounts for nonadministrators or separated administrators, exist. Specifically, we:
  - A. Compared all administrator user accounts to the IRS timekeeping system listing employee series, function, and status.
  - B. Identified potential nonadministrators and separated employees by comparing administrator lists to the timekeeping system, presenting and confirming the lists with local management, and, if applicable, identifying why administrator user accounts that were no longer needed had not been disabled or closed.

---

<sup>1</sup> The IRS uses the Information System User Registration/Change Request (Form 5081) to request and authorize user accounts for all systems. The OL5081 is an automated version of this Form. The OL5081 system was named after the Form 5081; it automates some of the manual processes and provides a centralized system for all system access authorizations.

<sup>2</sup> Appendix IV provides a description of these systems.



---

*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

- C. Identified any administrator user account(s) that had not been used for 60 calendar days and consulted with local management to determine whether there was any justification for the account(s).
- D. Determined whether administrator user accounts were regularly reviewed independently to identify inactive accounts and accounts no longer needed.
- III. Determined whether shared, generic, duplicate, or default accounts existed. Specifically, we reviewed system administrator user accounts for each application to identify accounts with possible shared, generic, duplicate, or default user account names and consulted with the administrators to determine why these types of accounts existed on the systems and whether reasonable justification existed for the accounts.
- IV. Determined whether applications contained strong password controls on system administrator user accounts. Specifically, we reviewed password settings files to determine whether settings were in compliance with IRS password policies and, if they were not, consulted with the administrators and managers to determine why the password controls had not been updated to reflect basic requirements.
- V. Determined whether system administrator activities were regularly reviewed independently for suspicious activities, computer configuration changes, and other potential security issues. We consulted with the independent reviewer to determine whether issues had been identified in the past, what the process was for handling those issues, and what the cause was of each issue.
- VI. Determined the causes for any conditions identified.



*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

**Appendix II**

*Major Contributors to This Report*

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)  
Stephen Mullins, Director  
Kent Sagara, Audit Manager  
Louis Lee, Lead Auditor  
Bret Hunter, Senior Auditor  
Jody Kitazono, Senior Auditor  
Abraham Millado, Senior Auditor



*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

**Appendix III**

*Report Distribution List*

Acting Commissioner C  
Office of the Commissioner – Attn: Acting Chief of Staff C  
Deputy Commissioner for Operations Support OS  
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 Liaison: Chief Information Officer OS:CIO



---

*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

---

## **Appendix IV**

### *Description of Internal Revenue Service Applications Selected for Review*

We selected the following five IRS applications for our review of system administrator user accounts:

**AIMS** – This System provides the inventory of and activity controls over active Examination Division cases for input on status changes, adjustments, and case-closing actions.

**ALS** – This System supports revenue officers in field offices by tracking lien assignments and lien due dates. It provides the abilities to print lien documents and to support management information reporting on liens, generates Notices of Federal Tax Liens and Releases of Liens, and maintains a database of all outstanding items.

**ASFR** – This System supports the automated selection of investigations on those taxpayers who have substantial reported income and yet refuse or neglect to file tax returns for a given year. It tracks all cases, issues required notices and results, and prepares a tax calculation summary that is mailed to the taxpayer.

**ELS** – This System enables tax examiners and clerks to review levies prior to printing and requires only levies with errors or those flagged from the Levy Review Register to be reviewed. The ELS eliminates time and paper costs associated with a manual review and the retyping of erroneous levies. The System also provides management with a variety of reports for volume, error, and trend analyses.

**ExFIRS** – This System provides management information and support processes to assess the health and direction of the Excise Tax Program. Multiple applications support Excise Tax Program business processes and internal/external stakeholder activities. There are approximately 550 IRS end users of the applications, in addition to State Excise Tax Agencies and the motor fuel industry.



*Effectiveness of Access Controls Over System Administrator  
User Accounts Can Be Improved*

**Appendix V**

*Management's Response to the Draft Report*



CHIEF INFORMATION OFFICER

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

RECEIVED

SEP - 4 2007

August 29, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard A. Spires  
Chief Information Officer

SUBJECT: Draft Audit Report – Effectiveness of Access Controls Over System  
Administrator User Accounts Can Be Improved  
(Audit #200620032) (i-trak #2007-27402)

Thank you for the opportunity to review and respond to the subject draft audit report. The IRS' Modernization and Information Technology Services (MITS) organization strives to protect the Service's computer systems by ensuring appropriate privileges and rights are assigned to employees by updating current policies, and by responding promptly and effectively to TIGTA recommendations.

We agree with and will implement all of your audit recommendations. We have attached our response to specific recommendations for system administration access controls and auditing of the system administrator activity.

Thank you for your continued support and guidance. We look forward to working with your staff to develop appropriate measures. If you have any questions, please contact me at (202) 622-6800. Members of your staff may also contact Perry Robinett, Director of Program Oversight Coordination, at (202) 283-6283.

Attachment



## *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

Attachment

Draft Audit Report – Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved (Audit #200620032) (i-trak #2007-27402)

**RECOMMENDATION #1:** To improve access controls over system administrator (SA) user accounts, we recommend the Chief Information Officer ensure that managers: Identify and reconcile SA user accounts on all systems to the OL5081 system. For those accounts not on the OL5081 system, the system owner and the SA's manager should determine whether the SA continues to have a business need for access. If the SA no longer has a business need, the SA user account should be deleted. If the SA continues to have a business need, the manager should initiate the process of creating an OL5081 record for the SA user account.

**CORRECTIVE ACTION #1:** We agree with the recommendation to improve access controls over system administrator user accounts by ensuring that managers identify and reconcile SA user accounts on all systems to the OL5081 system. The IRS will implement a process to review and compare System Administrator (SA) user accounts on all systems against the OL5081 system at least annually. For those SA user accounts not reflected on the OL5081 system, the SA's manager will consult with the SA and system owner to determine if there is a continuing business need for access. If the SA no longer has a need for access, the SA user account will be deleted. If the SA has a continuing need, the manager will initiate the process for creating an OL5081 record for the SA user account. The manager will delete the OL5081 record if it exists without an SA user account.

**IMPLEMENTATION DATE:** October 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Enterprise Operations

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION #2:** To improve access controls over SA user accounts, we recommend the Chief Information Officer ensure that managers: Test the automated computer programs (scripts) used to identify and disable SA user accounts with 45 days of inactivity and delete SA user accounts with 90 days of inactivity, and periodically validate the results to ensure the programs are working as intended.

**CORRECTIVE ACTION #2:** We agree with the recommendation to improve access controls over SA user accounts by ensuring that managers test the automated computer program (scripts) used to identify and disable SA user accounts with 45 days of inactivity and delete SA user accounts with 90 days of inactivity, and periodically validate the results to ensure the programs are working as intended. The IRS will implement the feature of the operating system to identify and delete all SA accounts with no activity in 45 days. An additional script will be added to all Unix systems to monitor, on a daily basis, the deactivated accounts for an additional 45 days. After 90 days of inactivity, the account will be removed and stored in a log. A systems review will be conducted quarterly to validate these automated processes are working as intended.

**IMPLEMENTATION DATE:** October 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Enterprise Operations



---

*Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

Attachment

Draft Audit Report – Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved (Audit #200620032) (i-trak #2007-27402)

---

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION #3:** To improve access controls over SA user accounts, we recommend the Chief Information Officer ensure that managers: Reinforce the need for managers of SAs to be cognizant of the applications their employees can access, and limit those access rights to only those applications needed to carry out their responsibilities. Managers should consider long periods of inactivity when determining whether to recertify access rights on the OL5081 system.

**CORRECTIVE ACTION #3:** We agree with the recommendation to improve access controls over SA user accounts, by ensuring that managers reinforce the need for managers of SAs to be cognizant of the applications their employees can access, and limit those access rights to only those applications needed to carry out their responsibilities. All SA managers will be sent a notice to reinforce their need to be aware of the applications their SAs can access and to limit those access rights to only those applications the SAs need to carry out their responsibilities. The notice will also remind managers to consider long periods of inactivity when determining whether to recertify access rights on the OL5081 system.

**IMPLEMENTATION DATE:** October 1, 2007

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Enterprise Operations

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION #4:** The Chief Information Officer should ensure the deployment of the host-based intrusion detection software continues to ensure audit trail reviews over SA user accounts on Tier 2 Unix-based servers.

**CORRECTIVE ACTION #4A:** We agree with the recommendation that the Chief Information Officer should ensure the deployment of the host-based intrusion detection software continues to ensure audit trail reviews over SA user accounts on Tier 2 Unix-based servers. Enterprise Operations (EOPS), in coordination with Cybersecurity, will deploy the Host-based Intrusion Detection Sensor (HIDS) agents on Tier 2 Unix-based servers.

**IMPLEMENTATION DATE:** December 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Enterprise Operations

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.



---

*Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved*

---

Attachment

Draft Audit Report – Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved (Audit #200620032) (i-trak #2007-27402)

---

**CA Milestones:**

Consolidated UNIX servers	June 1, 2008
Unconsolidated UNIX servers (OS upgrades)	December 1, 2008

Please note: This timeline will allow for determining the feasibility of implementing the Host-based Intrusion Detection Sensor (HIDS) agents on a variety of vendor operating system versions; some of which may not support operation of the HIDS, thus requiring an upgrade.

**CORRECTIVE ACTION #4B:** We agree with this recommendation that the Chief Information Officer should ensure the deployment of the host-based intrusion detection software continues to ensure audit trail reviews over SA user accounts on Tier 2 Unix-based servers. MITS' Cybersecurity organization is responsible for monitoring and reviewing the event logs. The deployment of HIDS software to the IRS' enterprise will capture event logs on Unix servers. HIDS will capture SA's user activities in the event log files. Cybersecurity's IT Security Field Specialists were trained in June and July 2007 to monitor the event logs, review HIDS reports, and alert the Computer Security Incident Response Center of unusual or suspicious activity. These IT Security Field Specialists will monitor the event logs to review the following HIDS Reports (on a weekly or as needed basis) as HIDS software is deployed enterprise-wide to new servers:

- Security Events by Category
- Attack Incidents Reports
- Top Attacks by Severity
- Asset Event Detail Report
- Top Attacks

All incidents will be captured and tracked in the Incident Tracking System.

**IMPLEMENTATION DATE:** December 1, 2008

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

**CORRECTIVE ACTION MONITORING PLAN:** Cybersecurity will monitor progress on this corrective action in the periodic (at least quarterly) compliance checks that are conducted by IT Security Field Specialists. The compliance check reports will specifically include checks to verify that audit event logs are being monitored and reviewed for all SA user accounts on Tier 2 Unix-based servers maintained by MITS or the business units, dependent on the overall MITS/EOPS project schedule for HIDS deployment on IRS servers, which is not expected to be completed until December 2008.