Computer System Access Controls Over Contractors Need to Be Improved

July 24, 2009

Reference Number: 2009-20-108

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:

3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 24, 2009

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Computer System Access Controls Over Contractors Need to Be Improved (Audit # 200820015)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) established and implemented effective computer access controls over contractors that have been hired to develop, operate, and maintain IRS computer systems. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan as part of the statutory requirements to annually review the adequacy and security of IRS information technology.

Impact on the Taxpayer

The IRS uses contractors to perform a variety of information technology functions, such as developing applications for IRS business operations and maintaining computer operations. To perform these functions, contractors are granted access to IRS computer systems. However, some contractors who no longer had a business need to have access had active user accounts on IRS systems. When contractors are allowed to have unnecessary access to computer systems, the IRS is increasing the risks of exposing taxpayer data to unauthorized disclosure and disruption of system operations.

Synopsis

We have previously reported[1] problems with contractors' access to IRS computer systems. The underlying theme of the problems is the IRS' inability to effectively control contractor access to its computer systems. One of the fundamental principles for effective computer security is restricting system access to only those systems for which individuals, including contractors, have a business need. The IRS has specific security policies and procedures governing access by employees and contractors to computer systems and taxpayer data.

Despite the IRS' policies and procedures and our previous reports of inadequate oversight of contractor access to IRS computer systems, we identified system access control issues for contractors. From a sample of 7 IRS systems, we found that 53 of 376 contractors had active user accounts but did not have a business need for access to that system. These 53 contractors consisted of contractors whose job duties or access privileges had changed and no longer needed system access, contractors who had separated from the contract with the IRS, and contractors who had never logged onto the system or had not logged onto the system within 45 calendar days. We also identified 15 contractors whose system access was not deleted in a timely manner upon separation from the contract with the IRS. These contractors' accesses were not removed from systems in a timely manner because responsible officials were not following security procedures and relied on systemic solutions to disable and delete user access to systems based on inactivity. Also, managers and Contracting Officer's Technical Representatives[2] did not provide the necessary oversight of reviewing access privileges and notifying system owners when contractors no longer needed access.

We also identified 12 system development contractors who had access to the production
3(d) environment of the system on which they worked and 39 system administration contractors who had database administrator privileges.

Lastly, we found system accesses were not always authorized, documented, or recertified in a timely manner, and system accesses were granted prior to a background investigation being completed. We believe managers and security officers did not carry out their security roles and responsibilities over system access.

---

[1] *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Reference Number 2004-20-063, dated March 22, 2004) and *Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved* (Reference Number 2005-20-185, dated September 29, 2005).

[2] Contracting Officer's Technical Representatives furnish technical direction, monitor contract performance, and maintain an arm's-length relationship with the contractor.

Recommendations

We recommended that the Chief Technology Officer 1) provide appropriate communications to all Contracting Officer's Technical Representatives and managers reinforcing the need to ensure that system accesses are revoked when contractors leave the IRS and that separation of duties is followed, 2) enforce current procedures on all systems by configuring systems to automatically disable and/or delete user accounts when they are not accessed for the appropriate number of days, 3) provide appropriate communications to all Contracting Officer's Technical Representatives and managers to remind them that they have the primary responsibility for providing prompt notification to the responsible organization of any contractor status changes, 4) provide appropriate communications to Contracting Officer's Technical Representatives and managers that the Online 5081 system is the primary system used for authorizing and approving requests for any system access and that system access should not be granted until a contractor or employee has successfully completed a background investigation, and 5) improve accountability over employee and manager adherence with security policies and procedures over contractor system access.

Response

IRS management agreed with the recommendations. The Modernization and Information Technology Services Cybersecurity organization will coordinate with the Agency-Wide Shared Services Contractor Oversight Group to develop and deliver appropriate communications content to Contractor Officer's Technical Representatives and managers that will 1) remind them of the notification responsibility, including annually reviewing access privileges to verify the continued need for access and, in accordance with existing IRS policy, suspending, cancelling, and/or adjusting contractor system access privileges; 2) address that after 45 calendar days have passed and the user is not recertified, procedures will be implemented to disable and remove or securely incapacitate the user account and access privileges; and 3) remind them of their obligation, in accordance with existing IRS policy, to separate contractors who do not adhere to security policies and procedures governing system access within 45 calendar days. Also, the Modernization and Information Technology Services organization will enforce system configuration settings to automatically disable contractors' accounts after 45 calendar days of inactivity and will ensure accounts that are inactive for more than 90 calendar days are deleted or securely incapacitated based on the technical capabilities and requirements of each system and platform. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

Table of Contents

Abbreviations

COTR	Contracting Officer's Technical Representative
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services
OL5081	Online 5081

Background

The Internal Revenue Service (IRS) relies extensively on contractors to provide information technology services and systems. These contractors perform a variety of information technology functions for the IRS, such as developing applications for business operations and maintaining computer operations. To perform these functions, contractors are granted access to IRS computer systems.

We have previously reported problems with contractors' access to IRS computer systems. In March 2004, we reported[1] that contractors were not complying with IRS security procedures and IRS Procurement function officials were not aware of the security regulations pertaining to the contractors they were assigned to oversee. In September 2005, we conducted a followup review[2] and identified that Procurement function officials were still not fulfilling their responsibilities related to granting contractors access to IRS systems. We identified more than 1,000 contractors who were no longer working for the IRS that could still sign on to IRS systems.

The underlying theme of these problems is the IRS' inability to effectively control contractor access to its computer systems. One of the fundamental principles for effective computer security is restricting system access to only those systems and applications for which individuals, including contractors, have a business need. This concept of need-to-know and least privilege includes having appropriate persons authorize system access, having program managers and systems owners monitor system access to ensure access is still needed based on job responsibilities, and removing system access when the need no longer exists.

This review was performed at the IRS National Headquarters in New Carrollton, Maryland, and in Modernization and Information Technology Services (MITS) organization field offices located in Atlanta, Georgia; Cincinnati, Ohio; Memphis, Tennessee; and Austin, Texas, during the period July 2008 through March 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Reference Number 2004-20-063, dated March 22, 2004).
[2] *Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved* (Reference Number 2005-20-185, dated September 29, 2005).

Results of Review

Contractors Had Unnecessary Access to Computer Systems

The IRS has specific security policies and procedures governing access by employees and contractors to computer systems and taxpayer data. However, our review identified two areas where contractors had unnecessary access to IRS computer systems and taxpayer data.

Contractors had active user accounts, but did not have a business need

The IRS has access control procedures and requirements that pertain to both IRS employees and contractors. These procedures include granting system access when the business need exists, applying the principles of need-to-know and least privilege, and taking away system access when the business need no longer exists. As a further control, the IRS requires disabling system access when no access has occurred within 45 calendar days and removing system access when no access has occurred within 90 calendar days.

Contractors are also subjected to further scrutiny from the Contracting Officer's Technical Representative (COTR),[3] who is responsible for the contract under which the contractor was hired to work. The COTR's duties include initiating access privileges for contractors, reviewing access privileges annually to verify the continued need for access, and notifying system owners in a timely manner when contractors no longer need access.

Despite these procedures, we identified contractors with active user accounts on IRS systems who no longer had a business need for that access. For a sample of 7 IRS systems, we identified that 53 (14 percent) of 376 contractors had active user accounts but did not have a business need for access to that system. We also identified five duplicate active user accounts for contractors on the systems we reviewed. The 53 contractors with active user accounts fell into the following exception categories:[4]

- *Job duties or access privileges changed and system access was no longer needed (35 contractors).* System owners and program managers were unaware of these situations when they occurred. COTRs did not know of the change in job duties or did not share the information with system owners or program managers.

[3] COTRs furnish technical direction, monitor contract performance, and maintain an arm's-length relationship with the contractor.
[4] The total number of exceptions is more than 53 because 4 contractors fell into more than 1 category.

- *Separated from the contract with the IRS (five contractors).* Of particular concern, we found that 3 of the 5 separated contractors left the IRS in May 2006, and the accounts were active and not used for more than 850 days. The IRS was unable to provide us any information on the separation dates for the other two contractors.
- *Never logged onto the system or had not logged onto the system within 45 calendar days (17 contractors).* This condition suggests that the contractors never needed access to the system in the first place or a change in needed access had occurred. Again, system owners and program managers were unaware of these situations, and COTRs did not know of the change in job duties or did not share the information with system owners or program managers.

In addition to contractors who had active system access with no business need, we identified 15 contractors whose system access was not deleted in a timely manner upon their separation from the IRS. The delays in removing system access ranged from 4 to 53 calendar days.

These contractors' accesses were not removed from systems in a timely manner because responsible officials were not following security procedures and relied on systemic solutions to disable and delete user access to systems based on inactivity. However, the automated programs to identify user accounts with inactivity were either not being run regularly or did not work as intended. Also, managers and COTRs did not provide the necessary oversight of reviewing access privileges and notifying system owners when contractors no longer needed access.

Contractors had excess privileges that violated separation of duties rules

Separation of duties is an organizational principle that provides process integrity while maintaining proper security and quality controls. IRS security policy states that system and application software development, testing, and debugging must be performed on information systems dedicated for these purposes and not on production information systems. To ensure proper separation of duties, system developers should not have access to the system's production environment. This separation ensures that system developers cannot make changes on production systems that have gone through rigorous testing and authorization to operate. Developers who have access to the production system could bypass strict configuration management requirements and make unapproved and untested changes. In addition, system administrators should not have database administrator privileges. While system administrators are responsible for the configuration and day-to-day operations of the system, the database administrators are responsible for the security, maintenance, and backup of the database repositories. This separation ensures the integrity of the data and that any unauthorized changes to the data can be detected.

We identified 12 system development contractors who had access to the production environment of the system on which they worked and 39 system administration contractors who had database administrator privileges. We were unable to determine how long these contractors had

unnecessary access to IRS production systems because we could not determine when these accounts were created, when contractors were given system access, or when user access privileges were granted or changed.

3(d) For the production environment access issue,

For the database administrator access issue,

3(d)

Two other factors have heightened our concerns about the access control deficiencies over contractors.

1. While we did not identify any questionable activity or wrongdoing by contractors who no longer had a business need for system access, our attempts to evaluate their activities were hampered by the lack of reviewable audit trail[5] data for the systems we reviewed. We referred this issue to an ongoing Treasury Inspector General for Tax Administration review over audit trails. Without the ability to monitor contractor system activities, the IRS is placed in the precarious position of relying on access controls as the sole means to ensure that contractors are accessing only the systems and data they require to do their jobs.
2. The IRS does not have an effective centralized system or method of identifying all contractors working within the IRS. This lack of accountability has hampered the IRS' ability to monitor contractors and control their computer system access. While the IRS has formed a committee to implement a central tracking process for contractors, the process is not in place and implementation efforts have encountered difficulties.

When contractors are allowed to have unnecessary access to IRS systems and taxpayer data, the IRS is increasing the risks of exposing taxpayer data to unauthorized disclosure and disruption of system operations. All seven computer systems in our review contain taxpayer data, including taxpayer correspondence; current, past, and questionable tax returns; delinquent taxpayer accounts; and fuel transaction information on billing and vehicle registration.

To illustrate these risks, several news outlets published a January 2009 news story relating to a former Federal National Mortgage Association (Fannie Mae) information technology contractor who was indicted for installing a malicious computer program that would have caused millions of dollars of damage and reduced, if not shutdown, operations at the mortgage giant. The malicious program would have disabled monitoring alerts and logins, deleted root passwords to 4,000 servers, and erased all data and backup data on those servers by overwriting them with zeros. However, the malicious program was discovered by an employee 5 days after it was

[5] An audit trail is a chronological record of activities that allow for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to computer networks.

installed, and no actual harm occurred. The contractor was able to install the malicious program because his system access privileges were not revoked as soon as he was terminated from his position. An equally disturbing possible outcome, as noted in comments from a reader to one of the online news articles, was that the contractor could have stolen critical customer data for the purpose of monetary gain instead of attempting to disrupt computer operations.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Provide appropriate communications to all COTRs and managers reinforcing the need to ensure appropriate system accesses are revoked when contractors leave the IRS and contractors' duties no longer require system access, and that separation of duties is followed to ensure that contractors do not have access to both development and production system environments and do not have both system and database administrator privileges.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS Cybersecurity organization will coordinate with the Agency-Wide Shared Services Contractor Oversight Group to develop and deliver appropriate communications content to COTRs.

Recommendation 2: Enforce current procedures on all systems by configuring systems to automatically disable contractors' accounts after 45 calendar days of inactivity and to delete the accounts after 90 calendar days of inactivity.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS organization will enforce system configuration settings to automatically disable contractors' accounts after 45 calendar days of inactivity and will ensure that accounts that are inactive for more than 90 calendar days are deleted or securely incapacitated based on the technical capabilities and requirements of each system and platform. Securely incapacitating accounts will effectively delete all access capability while retaining account background information. Current procedures will be reviewed and updated to ensure that the associated technical configurations are appropriately documented.

Recommendation 3: Provide appropriate communications to all COTRs and managers to remind them that they have the primary responsibility for providing prompt notification to the responsible organization of any contractor status changes, including annually reviewing access privileges to verify the continued need for access. The responsible organization should immediately suspend, cancel, and/or adjust all access privileges associated with changes in a contractor's status.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS Cybersecurity organization will coordinate with the Agency-Wide Shared Services

Contractor Oversight Group to provide appropriate communications to COTRs and managers reminding them of this notification responsibility, including annually reviewing access privileges to verify the continued need for access and, in accordance with existing IRS policy, suspend, cancel, and/or adjust contractor system access privileges.

Compliance With Security Requirements Could Be Improved for Contractors Who Have a Business Need for System Access

The IRS has specific procedures and requirements for authorizing system access for employees and contractors. Our review identified two areas where access authorization controls over contractors can be improved.

System accesses were not always authorized, documented, or recertified in a timely manner

Providing contractors access to IRS computer systems starts with the system access authorization process. The IRS established the Information System User Registration/Change Request (Form 5081) for managers to request and authorize employee and contractor access for all IRS systems, including development and production systems. System administrators are responsible for adding and removing authorized system users and maintaining an up-to-date list of authorized users. In October 2002, the IRS automated the system authorization process with the Online 5081 (OL5081) system. The OL5081 system also provides documentation information on a contractor's certification that he or she understands the IRS security rules over computer usage and on the manager's annual recertification of the contractor's continued system access and need-to-know.

The IRS also established other complementary security controls. Managers are required to annually review users' accounts and profiles, including a review of the access level, conformance with the principle of least privilege, and current management authorizations.

Even though clear security policies and procedures have been established, we identified that 46 (12 percent) of 376 contractor accounts did not have proper authorization for system access on the OL5081 system. We were also unable to find paper copies of approved authorizations from the contractors' current managers or COTRs. Twenty-four of the 46 contractor accounts are associated with a development system, which operated with live taxpayer data and had not received an approved waiver to operate in this condition.

For one development system, the IRS manager over the system informed us that, because it was a development system, access was granted using email instead of using the OL5081 system. For the other systems without the Form 5081 information, we were unable to determine how these contractors obtained access to the systems. We believe that managers either did not carry out their responsibilities to follow approved system access authorization processes or system administrators may have added contractors to systems without a manager's authorization. The

IRS confirmed that those contractors needing access to IRS systems were in the process of completing system access authorization.

We also identified 39 (21 percent) of 187[6] contractor accounts that were not recertified in a timely manner by a manager to indicate that the contractors had a continued need for system access. We were informed that contractor system accesses were not recertified in a timely manner because:

- Managers were busy and did not have time to recertify the contractor's continued system access and need-to-know.
- A transition in managers caused confusion over which manager should do the recertification.
- Managers were uncertain whether there was still a business need for system access and required more time to make a determination.
- Managers of contractors whose access were granted using a paper Form 5081 did not receive electronic email reminders to recertify.

System accesses were granted prior to a background investigation being completed

IRS policy requires that a background investigation must be conducted on employees and contractors at the risk level appropriate to the sensitivity of the position before system access is granted. At a minimum, contractors should not be given access to sensitive IRS systems until they have a completed background investigation or have received interim access approval. The background investigation provides a level of assurance that the employee or contractor is of good character and can be trusted with access to sensitive data.

Despite this requirement, we found that 7 (2 percent) of 376 contractors were given system access prior to a background investigation being completed or their receiving interim access approval. We believe managers and security officers did not carry out their responsibilities of verifying whether a background investigation was completed or that the contractor had received interim access approval before granting the contractor system access. All seven contractors eventually had a completed background investigation.

When contractors are allowed to have access to IRS systems before the completion of system access authorization tasks, the IRS increases its risk of unauthorized access to taxpayer data as well as personally identifiable information.

[6] The 187 contractor accounts represent those user accounts in our sample where access was granted over 1 year prior to system access and were, therefore, subject to annual recertification requirements.

Recommendations

The Chief Technology Officer should:

Recommendation 4: Provide appropriate communications to all COTRs and managers that the OL5081 system is the primary system used for authorizing and approving requests for any system access. System access should not be granted until the contractor or employee has successfully completed a background investigation and been approved for access through the OL5081 system. Managers and COTRs have the primary responsibility to ensure that contractors and employees complete their annual certification requirements within 45 calendar days of notification. If after 45 days have passed and a user has not recertified, the System Administrator should disable and remove the user account and access privileges from the system.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS Cybersecurity organization will coordinate with the Agency-Wide Shared Services Contractor Oversight Group to develop and deliver appropriate communications content to COTRs. In addition, the communication will also address that after 45 calendar days have passed and the user is not recertified, procedures will be implemented to disable and remove or securely incapacitate the user account and access privileges.

Recommendation 5: Ensure that COTRs understand their obligation to separate contractors who do not adhere to security policies and procedures governing system access within 45 calendar days. In cases where a COTR does not separate a noncompliant contractor, notification should be provided to the COTR's manager that the manager needs to direct the COTR to separate the contractor. If the COTR still fails to separate the contractor, the manager should take appropriate action.

> ***Management's Response:*** The IRS agreed with this recommendation. The MITS Cybersecurity organization will coordinate with the Agency-Wide Shared Services Contractor Oversight Group to provide appropriate communications to COTRs reminding them of their obligation, in accordance with existing IRS policy, to separate contractors who do not adhere to security policies and procedures governing system access within 45 calendar days. This notification will also reinforce taking the appropriate actions when this obligation is not fulfilled.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS established and implemented effective computer access controls over contractors that have been hired to develop, operate, and maintain IRS computer systems. To accomplish this objective, we:

I. Determined whether the IRS is effectively controlling contractor access.

A. Identified systems with contractor user accounts and judgmentally selected 7 of 65 systems, totaling 376 contractor user accounts, for review based on the number of contractor user accounts and the sensitivity and location of the systems. The seven systems selected for review were: the Excise Files Information Retrieval System in Cincinnati, Ohio; the Electronic Fraud Detection System and the Integrated Collection System in Memphis Tennessee; the Correspondence Imaging System–Development, Correspondence Imaging System–Application, and Correspondence Imaging System–Imaging in Austin, Texas; and the Integrated Data Retrieval System in Atlanta, Georgia, and Austin, Texas.

B. Determined whether contractors' access rights were authorized for each system selected for review. We obtained a download from the OL5081 system of contractor accounts for the systems selected. We verified this information by requesting a download from each system selected and reconciled this information to the Treasury Integration Management Information System[1] database for current and separated employees. Those accounts not matched were identified as contractor accounts and reconciled with the OL5081 data.

C. Determined whether contractors' managers recertified annually their continued need-to-know for system access. Only 187 of 376 contractor accounts represented those user accounts where access was granted over 1 year from system access and were subject to recertification requirements.

D. Determined whether contractors received the proper level of background investigation prior to system access.

E. Reviewed contractor account information to identify periods of inactivity.

F. Determined whether contractors have a continued need-to-know for system access.

[1] An official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. It is outsourced to the United States Department of Agriculture National Finance Center and managed by the Department of the Treasury.

G. Determined whether developers have access to live data and production systems.

H. Determined the causes for any conditions identified above.

I. Reviewed audit trails[2] for fraud indicators and trends.

II. Determine whether contractors are complying with IRS security policies and procedures.

A. Identified applicable security policies and procedures.

B. Determined whether contractors violated security policies and procedures.

C. Determined the causes for contractors not complying with IRS policies and procedures for handling sensitive IRS data.

D. Assessed the effect of the inadequate security controls identified above.

[2] An audit trail is a chronological record of activities that allow for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to computer networks.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Acting Director
Jody Kitazono, Acting Audit Manager
Louis Lee, Lead Auditor
Alan Beber, Senior Auditor
Myron Gulley, Senior Auditor
Abraham Millado, Senior Auditor
Larry Reimer, Senior Auditor
Stasha Smith, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Stakeholder Management Division OS:CTO:SM
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 Technology Officer OS:CTO

Appendix IV

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

July 14, 2009

RECEIVED
JUL 14 2009

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Computer System Access Controls Over Contractors Need to Be Improved (Audit #200820015) (i-trak #2009-59662)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. We appreciate your comments and observations on actions the Internal Revenue Service can take to improve computer access controls over contractors.

The Service's Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes and your suggested recommendations will further help improve our security posture. We agree with all of the report recommendations made as a result of your audit. The attachment to this memo details our planned corrective actions to implement the recommendations.

Your continued support and the assistance and guidance your team provides have been a valuable resource to our organization. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment

Attachment

Draft Audit Report – Computer System Access Controls Over Contractors Need to Be Improved (Audit #200820015) (i-trak #2009-59662)

RECOMMENDATION #1: The Chief Technology Officer should provide appropriate communications to all COTRs and managers reinforcing the need to ensure appropriate system accesses are revoked when contractors leave the IRS and contractors' duties no longer require system access, and that separation of duties is followed to ensure that contractors do not have access to both development and production system environments and do not have both system and database administrator privileges.

CORRECTIVE ACTION #1: We agree with this recommendation. The Modernization and Information Technology Services' Cybersecurity organization will coordinate with the Agency Wide Shared Services' Contractor Oversight Group to develop and deliver appropriate communications content to Contracting Officer Technical Representatives (COTRs).

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #2: The Chief Technology Officer should enforce current procedures on all systems by configuring systems to automatically disable contractors' accounts after 45 days of inactivity and to delete the accounts after 90 days of inactivity.

CORRECTIVE ACTION #2: We agree with this recommendation. The Modernization and Information Technology Services (MITS) organization will enforce system configuration settings to automatically disable contractor's accounts after 45 days of inactivity. MITS will ensure accounts inactive for more than 90 days are deleted or securely incapacitated based on technical capabilities/requirements of each system/platform. Securely incapacitating accounts will effectively delete all access capability while retaining account background information. Current procedures will be reviewed and updated to ensure the associated technical configurations are appropriately documented.

IMPLEMENTATION DATE: March 1, 2010

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) and monitor them on a monthly basis until completion.

Attachment

Draft Audit Report – Computer System Access Controls Over Contractors Need to Be Improved
(Audit #200820015) (i-trak #2009-59662)

RECOMMENDATION #3: The Chief Technology Officer should provide appropriate communications to all COTRs and managers to remind them that they have the primary responsibility for providing prompt notification to the responsible organization of any contractor status changes, including annually reviewing access privileges to verify the continued need for access. The responsible organization should immediately suspend, cancel and/or adjust all access privileges associated with changes in a contractor status.

CORRECTIVE ACTION #3: We agree with this recommendation. The Modernization and Information Technology Services' Cybersecurity organization will coordinate with the Agency Wide Shared Services' Contractor Oversight Group, to provide appropriate communications to COTRs and managers reminding them of this notification responsibility, including annually reviewing access privileges to verify the continued need for access, and in accordance with existing IRS policy, suspend, cancel, and/or adjust contractor system access privileges.

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Technology Officer should provide appropriate communications to all COTRs and managers that the OL5081 system is the primary system used for authorizing and approving requests for any system access. System access should not be granted until the contractor or employee has successfully completed a background investigation and been approved for access through the OL5081 system. Managers and COTRs have the primary responsibility to ensure that contractors and employees complete their annual certification requirements within 45 days of notification. If after 45 days have passed and a user has not recertified, the System Administrator should disable and remove the user account and access privileges from the system.

CORRECTIVE ACTION #4: We agree with this recommendation. The Modernization and Information Technology Services' Cybersecurity organization will coordinate with the Agency Wide Shared Services' Contractor Oversight Group to develop and deliver appropriate communication content to Contracting Officer Technical Representatives. In addition, being consistent with IRS procedure in corrective action #2, the communication will also address that after 45 days have passed and the user is not recertified, procedures will be implemented to disable and remove or securely incapacitate the user account and access privileges.

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Computer System Access Controls Over Contractors Need to Be Improved (Audit #200820015) (i-trak #2009-59662)

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

RECOMMENDATION #5: The Chief Technology Officer should ensure that COTRs understand their obligation to separate contractors who do not adhere to security policies and procedures governing system access within 45 calendar days. In cases where the COTR does not separate a non-compliant contractor, notification should be provided to the COTR's manager that the manager needs to direct the COTR to separate the contractor. If the COTR still fails to separate the contractor, the manager should take appropriate action.

CORRECTIVE ACTION #5: We agree with the intent of this recommendation. The Modernization and Information Technology Services' Cybersecurity organization will coordinate with the Agency Wide Shared Services' Contractor Oversight Group, to provide appropriate communications to Contracting Officer Technical Representatives reminding them of their obligation in accordance with existing IRS policy, to separate contractors who do not adhere to security policies and procedures governing system access within 45 calendar days. This notification will also reinforce taking the appropriate actions when this obligation is not fulfilled.

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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