Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved

September 2005

Reference Number: 2005-20-185

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 29, 2005

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE AND SECURITY SERVICES
DIRECTOR, PROCUREMENT

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved (Audit # 200520002)

This report presents the results of our review of the monitoring of contractor access to networks and data. The overall objective of this review was to determine whether Internal Revenue Service (IRS) management implemented adequate controls over the PRIME contractor's[1] access to IRS networks and data.

The IRS has about 900 contracts with private contractors. Many of these contractors must be given access to IRS computer systems and taxpayer data to complete their tasks, particularly those tasks that involve developing sensitive computer systems and providing computer hardware and software. In accordance with the Federal Information Security Management Act (FISMA),[2] contractors are subject to the same security standards, guidelines, and oversight that are required for Federal Government agencies. Without adequate oversight by the IRS, there is a significant risk of misuse or disclosure of confidential data as well as possible sabotage to these critical systems.

In March 2004, we reported[3] that contractors were not complying with certain IRS security procedures and IRS procurement officials were not aware of the security regulations pertaining

[1] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.
[2] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[3] *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Reference Number 2004-20-063, dated March 2004).

to the contractors they were assigned to oversee. In this audit, we followed up on prior recommendations and focused on work performed by the PRIME contractor.

Synopsis

During Calendar Year 2004, PRIME contractor personnel claimed they were not being granted timely access to systems, which affected their ability to efficiently perform their duties. As a result, the IRS gave the PRIME contractor the authority to add, delete, and modify its own employees' user accounts on IRS systems. Our review showed that the PRIME contractor added 199 user accounts without any oversight by the IRS during this 1-year period. The IRS, by allowing the PRIME contractor to approve access for its own employees with no oversight, did not comply with the FISMA.

In January 2005, to regain control of the PRIME contractor's access to IRS systems and data, the IRS assigned an employee to review all requests for PRIME contractor personnel to be added to or deleted from IRS systems. However, access was granted solely on the request of the PRIME contractor with no justification required. We do not believe it is feasible to place this responsibility with one person who could not possibly be aware of the PRIME contractor's access needs for each contract.

IRS procurement officials, specifically Contracting Officer's Technical Representatives (COTR), should be responsible for granting contractor employees access to IRS systems. Our findings in this audit indicate these Procurement function officials are still not fulfilling their responsibilities. More actions are needed to ensure contractors' access to IRS systems is limited to those who need it to accomplish their responsibilities and is monitored to detect any unauthorized activity.

The IRS worked with the PRIME contractor during January 2005 to identify over 1,000 separated contractor employees who no longer needed access but who could still sign on to IRS systems. As of May 2005, most of these accounts had been deactivated, but 160 of these contractor employees still had access to IRS systems.

We also found no documentation to indicate the IRS was monitoring the activities of PRIME contractor employees when they were accessing IRS systems. As a result, the risk of undetected security violations is increased. A security specialist stated that audit trails are reviewed; however, the reviews are not documented.

The PRIME contractor has remote access to the IRS network so it can perform much of its systems development and test procedures from its offices in the Maryland Technology Center in New Carrollton, Maryland. We determined the data link between the PRIME contractor's offices and the IRS was properly encrypted and physical security at the Maryland Technology Center was adequate.

Recommendations

We recommended the Chief Information Officer, in coordination with the Director, Procurement, ensure procurement officials obtain sufficient justification from the PRIME contractor before network access is granted. Also, a quarterly review of the active access account list should be performed to ensure accounts no longer needed are promptly disabled. In addition, the Chief, Mission Assurance and Security Services, should ensure audit trail reviews of contractor activity are conducted as prescribed by IRS procedures.

Response

The IRS agreed with our recommendations. Management stated a Memorandum of Understanding has been drafted outlining the roles and responsibilities of each office involved in ensuring contractor personnel gain access to only those systems needed to perform their work. A list of applications needed by contractors will be provided for each PRIME contractor project and will be used by the IRS to determine whether contractors' access requests should be granted. The Director, Procurement, will require the PRIME contractor to submit a list of terminated employees and an active account list quarterly. The IRS COTR will identify any accounts that are no longer needed, and the PRIME System Access Manager will deactivate those accounts.

The Chief, Mission Assurance and Security Services, stated that all contractor activities in the PRIME contractor test and development environment will be subject to the same monitoring tools used on any IRS processing environment. In addition, specific instructions will be sent to administrators of production environment systems directing them to include a review of user access from the PRIME contractor test and development environment as a key component of their standard system auditing activities. 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, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

The Internal Revenue Service (IRS) has about 900 contracts with private contractors. Many of these contractors must be given access to IRS computer systems and taxpayer data to complete their tests, particularly those tasks that involve developing sensitive computer systems and providing hardware and software. In accordance with the Federal Information Security Management Act (FISMA),[1] contractors are subject to the same security standards, guidelines, and oversight that are required for Federal Government agencies. Without adequate oversight by the IRS, there is a significant risk of misuse or disclosure of confidential data as well as possible sabotage to these critical systems.

In this audit, we focused on work performed by the PRIME contractor[2] for the IRS. PRIME contractor employees have access to critical equipment and systems to perform their duties. We evaluated the hardware and software access privileges, authentication requirements, monitoring of PRIME contractor activities, and security of connections between the PRIME contractor and the IRS computer systems. We also evaluated the physical security for one contractor-owned work facility that contained a computer network with access to the IRS enterprise network.

This review was performed in the Modernization and Information Technology Services (MITS) organization offices at the Martinsburg Computing Center[3] in Martinsburg, West Virginia, and the contractor-owned Maryland Technology Center (MTC)[4] in New Carrollton, Maryland, during the period November 2004 through May 2005. 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.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.
[3] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[4] The MTC, located adjacent to the New Carrollton Federal Building in New Carrollton, Maryland, is the principal site at which the PRIME contractor develops and tests systems to support the IRS' modernization efforts.

Results of Review

Accesses to Systems Were Not Properly Authorized

To reduce the risks of unauthorized access to Federal tax information, the IRS requires that access to sensitive systems be limited to only those persons needing it to carry out their responsibilities. The IRS requires employees to be formally authorized by a manager before accessing sensitive systems. For contractor personnel, the need to access sensitive systems must first be acknowledged by an IRS Contracting Officer's Technical Representative (COTR) who is responsible for overseeing contractor activities. The COTR should then prepare the documentation to provide the contractor with access to the necessary IRS systems.

Authorizations for PRIME contractor accesses were not properly granted

During Calendar Year 2004, the IRS granted proxy rights to the PRIME contractor that allowed it to add, delete, and modify its own employees' user accounts on IRS systems. The Business Systems Modernization function of the MITS organization made this decision in response to a claim by PRIME contractor personnel that they were not being granted timely access to systems, which affected their ability to efficiently perform their responsibilities.

The PRIME Contractor was granting access to its own employees with no oversight by the IRS.

We reviewed accesses granted for applications[5] used by the PRIME contractor during 2004. Of the 423 PRIME contractor personnel with user accounts for these applications, we identified:

- User accounts added by the PRIME contractor without any approval or oversight by an IRS COTR or manager (128 user accounts).
- User accounts added without any approval from an IRS COTR or manager or from the PRIME contractor (71 user accounts). Of the 71 user accounts, 52 were supported by an

[5] We reviewed accesses for the Inventory Tracking Asset Management System (ITAMS) and the Integrated Financial System (IFS) applications. The ITAMS provides tracking information on computer assets. The IFS provides detailed financial, cost accounting, property accounting, and procurement data to authorized users. The IFS Release 1 implements the core processes of general ledger, accounts payable, accounts receivable, budget execution, cost accounting, administrative tax and travel accounting, cost performance management allocations, some tax processing functionality, budget formulation, and budget execution decision support.

unsigned Information System User Registration/Change Request (Form 5081). The IRS had no documentation to show the other 19 user accounts had been added.

As a result, we could not determine who added the accounts to the systems or whether the need for access was justified. The access decisions were made solely by the PRIME contractor. The PRIME contractor managers given responsibility for granting access could not provide justification for those decisions. We are coordinating with the COTRs responsible for overseeing contractor activities on the systems used by the PRIME contractor during 2004 to determine whether accesses by contractor personnel were justified.

In January 2005, to regain control of the PRIME contractor's access to IRS systems and data, the IRS appointed a MITS organization employee as the PRIME System Access Manager, to review all requests for PRIME contractor personnel to be added to or deleted from IRS systems. In the first 6 months after procedures were changed, 24 contractor personnel accounts were added to various applications. For each of the 24 accounts, access was granted by the PRIME System Access Manager without acknowledgement from a COTR that access was needed. Accesses were granted solely on the request of the PRIME contractor with no justification as to the need for access. As a result, the IRS Manager granting access did not have sufficient information to determine whether the PRIME contractor employees needed access to complete their work or whether the level of access being granted was proper for the work to be completed. We do not believe it is feasible to place this responsibility with one person who could not possibly be aware of the PRIME contractor's access needs on each contract.

In March 2004, we reported[6] that contractors were not complying with certain IRS security procedures and IRS COTRs were not aware of the security regulations pertaining to the contractors they were assigned to oversee. In that report, we recommended the Chief, Mission Assurance and Security Services, and the Chief, Agency-Wide Shared Services, ensure the COTRs carry out their responsibilities to periodically review contractor compliance with established security policies. Management's response stated the Mission Assurance and Security Services organization would review and update guidance for Contracting Officers and COTRs on applicable security policies. This guidance was distributed to the COTRs to assist them in monitoring contractor activities.

Our findings in this audit indicate that COTRs are still not fulfilling their responsibilities to review contractor compliance with established security policies. More actions are needed to ensure contractors' access to IRS systems is limited to those who need it to accomplish their responsibilities and is monitored to detect any unauthorized activity.

In addition, the decision by Business Systems Modernization management to allow the PRIME contractor to approve access for its own employees with no oversight from the IRS is contrary to

[6] *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Reference Number 2004-20-063, dated March 2004).

FISMA guidance. FISMA Section 3544(b) requires each agency to provide security over "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." The Office of Management and Budget (OMB) also states agencies must develop policies for information security oversight of contractors and must review the security of other users with privileged access to Federal Government data and systems.[7]

PRIME contractor user accounts were not removed when access was no longer required

In January 2005, the IRS Procurement function asked the PRIME contractor to identify its personnel who had either separated from the PRIME contractor or no longer worked on any of the applications reviewed but could still sign on to IRS systems. The PRIME contractor identified 1,045 of its employees meeting these specifications. As of May 2005, most of these accounts had been deactivated, but 160 of these contractor employees still had access to IRS systems, increasing the risk of unauthorized disclosures and disruptions of operations. The IRS requires that accounts be deactivated when there is no longer a business need to access an IRS system. The PRIME contractor did not comply with this requirement, and the IRS did not provide sufficient oversight to ensure PRIME contractor user accounts were promptly disabled when no longer needed.

Monitoring of PRIME contractor activity was not sufficient to determine whether data were properly secured

IRS policies require system activity to be monitored by producing and reviewing audit trail data. We found no documentation to indicate the IRS personnel responsible for the security of computer systems are reviewing audit trails on computers used by the PRIME contractor. As a result, the risk of undetected security violations is increased. The security specialist stated that audit trail data are reviewed; however, the reviews are not documented.

We found no documentation that contractor activities on the IRS network are being monitored.

[7] *Fiscal Year 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (OMB Memorandum M05-15, dated June 13, 2005).

Recommendations

Recommendation 1: The Chief Information Officer, in coordination with the Director, Procurement, should ensure COTRs obtain sufficient documentation from the PRIME contractor to justify access to IRS systems. Before granting access to a contractor employee, the PRIME System Access Manager should obtain acknowledgement from the respective COTR that the access is needed.

> ***Management's Response:*** Management agreed with this recommendation, stating that a Memorandum of Understanding has been drafted outlining the roles and responsibilities of each office involved in the process of ensuring contractors gain access to only those systems needed to perform their work. A list of applications needed by contractors will be provided for each PRIME project and will be used by the IRS to determine whether contractors' access requests should be granted.

Recommendation 2: The Chief Information Officer, in coordination with the Director, Procurement, should require the PRIME System Access Manager to review the active account list quarterly for all applications used by the PRIME contractor to ensure accounts no longer needed are promptly disabled.

> ***Management's Response:*** Management agreed with this recommendation. The Director, Procurement, will require the PRIME contractor to submit a list of terminated employees and an active account list quarterly. The IRS COTR will identify any accounts that are no longer needed, and the PRIME System Access Manager will deactivate those accounts.

Recommendation 3: The Chief, Mission Assurance and Security Services, should ensure audit trail reviews of contractor activity are conducted as prescribed by IRS procedures.

> ***Management's Response:*** Management agreed with this recommendation. The Chief, Mission Assurance and Security Services, stated that all contractor activities in the PRIME contractor test and development environment will be subject to the same monitoring tools used on any other IRS processing environment. In addition, specific instructions will be sent to administrators of production environment systems directing them to include a review of user access from the PRIME contractor test and development environment as part of their standard system auditing activities.

Data Transfers Were Properly Encrypted

The PRIME contractor has remote access to the IRS network so it can perform much of its systems development and test procedures at its offices in the MTC. The National Institute of

Standards and Technology has determined that sensitive data should be encrypted if they are vulnerable to unauthorized disclosure. IRS policy requires that encryption shall be used for transmitting sensitive but unclassified information among IRS facilities and between the IRS and other facilities.

We determined the data link between the PRIME contractor's offices and the IRS was properly encrypted. We confirmed the software needed to encrypt and decrypt data transmitted between the two sites was in place and functioning. As a result, the risk that data being transmitted between them could be intercepted was adequately reduced.

Physical Security at the Maryland Technology Center Was Adequate

We reviewed the adequacy of physical security at the MTC by inspecting all closets and work areas to determine whether they were secure and accessible only to authorized individuals. The IRS requires that access to secure areas be closely monitored to prevent access by unauthorized personnel. Access to these areas was controlled by the use of keycards and security cameras on each floor containing IRS hardware.

Our test of the external perimeter of the facility showed the following three security weaknesses:

- The security guards did not request identification or ask that vendors sign in and out at the front gate when entering or exiting the facility.
- The door to the MTC docking area leading into the facility was ajar.
- A door adjacent to the docking area leading into the facility was ajar.

We informed MTC security personnel of these conditions and explained that a person with malicious intentions could enter through the front gate without being documented and proceed from the docking area into the MTC facility. The security personnel concurred with our assessment and immediately began a logging procedure for guests and vendors entering through the front gate area. In addition, an alarm was installed on the door leading to the docking area that would activate when the door was inappropriately accessed. With these changes in place, we found that physical security at the MTC was adequate. No other corrective actions are recommended.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether Internal Revenue Service (IRS) management implemented adequate controls over the PRIME contractor's[1] access to IRS networks and data. We evaluated the hardware and software access privileges, authentication requirements, audit trail collection and review, and security of connections between the PRIME contractor and the IRS computer systems. We also evaluated the physical security for one contractor-owned work facility that contained a computer network with access to the IRS enterprise network. We also followed up on prior recommendations contained on our report dated March 2004.[2] Specifically, we:

I. Determined whether the PRIME contractor's access permissions to IRS networks were limited to those employees who needed it to execute their responsibilities.

   A. For Calendar Year 2004, determined whether user access was authorized by verifying whether each contractor employee assigned to two specific applications had an Information System User Registration/Change Request (Form 5081) on file for the system on which he or she was listed as a user. We chose the two applications because they were accessed most frequently by contractor personnel during Calendar Year 2004.

   B. Obtained a listing from the system administrator of users on the system who have not accessed the system within 45 days and 90 days. We determined whether the accounts were automatically locked.

   C. Determined the IRS' and the PRIME contractor's role in granting network access to the PRIME contractor.

      1. Determined how the appropriate managers verify that the required background investigation has been initiated or completed.

      2. Determined whether an Online Form 5081 was used and if this was mandatory, the contractor's access privileges were correct, and anyone in the IRS questioned the contractor's need for administrative privilege.

[1] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.
[2] *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Reference Number 2004-20-063, dated March 2004).

3. Determined how a system administrator knows when to remove system access for a separated or transferred contractor employee.

II. Determined the extent of the IRS' review of audit logs of contractor-used computers at the two locations, the Maryland Technology Center (MTC)[3] and the Martinsburg Computing Center.[4]

A. Determined who performed the review of audit logs of PRIME contractor computers and how often the reviews were performed.

B. Attempted to secure copies of any reports on audit logs for computers used by PRIME contractor employees; any reports showing the corrective actions taken because of the monitoring of the audit logs; and any incident reports that were elevated to a higher level of management or to the IRS Computer Systems Incident Response Center, which provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise. The IRS could not provide any of the audit log reports.

III. Determined the level of physical security at the MTC using the National Institute of Standards and Technology (NIST) *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26).[5]

A. Determined whether access to facilities was controlled through the use of guards, identification badges, and entry devices such as key cards, biometrics, and locks; management periodically reviewed the list of persons with physical access to the facility; emergency exit and reentry procedures ensured only authorized personnel were allowed to reenter after fire drills, etc.; and visitors to sensitive areas were required to sign in and were escorted.

B. Determined whether physical accesses were monitored through audit trails, apparent security violations were investigated and remedial actions taken, and suspicious access activity was investigated and appropriate actions were taken.

C. Determined whether visitors, contractors, and maintenance personnel were authenticated with preplanned appointments and identification checks.

[3] The MTC, located adjacent to the New Carrollton Federal Building in New Carrollton, Maryland, is the principal site at which the PRIME contractor develops and tests systems being developed to support the IRS' modernization efforts.
[4] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[5] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

IV. Determined whether data transfers between the IRS and the PRIME contractor were encrypted and adequately secured.

A. Verified the methods used to transfer data files between the IRS network and PRIME contractor personnel by physically observing file transfers.

B. Ascertained the protocols used and obtained an explanation of the security features of those protocols.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Gerald Horn, Audit Manager
David Brown, Senior Auditor
William Lessa, Senior Auditor
Thomas Nacinovich, Senior Auditor
William Simmons, 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
Deputy Commissioner for Service and Enforcement SE
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 Management Controls OS:CFO:AR:M
Audit Liaisons:
- Chief Information Officer OS:CIO
- Chief, Mission Assurance and Security Services OS:MA
- Director, Procurement OS:A:P

Appendix IV

Management's Response to the Draft Report

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

RECEIVED
SEP 21 2005

CHIEF
MISSION ASSURANCE

September 20, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel Galik D. Galik
Chief, Mission Assurance and Security Services

SUBJECT: Management Response to Draft Audit Report: Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved (Audit # 200520002) (ECMS- 0508-6FKQ65YC)

Security at the Internal Revenue Service (IRS) is a top priority. The IRS requires that access to sensitive information systems be limited to only those persons with a need to execute their responsibilities. For contractor personnel, the need to access sensitive information systems is confirmed by an IRS Contracting Officer's Technical Representative (COTR) who is responsible for overseeing contractor activities. The COTR prepares the documentation to provide the contractor with access to the necessary IRS systems.

Your audit focused on the PRIME contractor for the IRS, which is an alliance of leading technology companies to assist with the IRS' efforts to modernize its computer systems and related information technology. We are pleased that your draft report acknowledges some of the work conducted by the IRS and the PRIME contractor between January and May 2005 to identify and deactivate accounts of separated contractor employees who no longer needed access to IRS systems.

Specifically, improvement actions began in early 2004 and continued throughout the year to address gaps in the PRIME contractor enrollment and the 5081 processes and to deal with a large backlog of PRIME access requests. For example, members of my staff and the Business Systems Modernization Office (BSMO) have been working on improving the process for the On-line (OL) applications for systems accesses. As mentioned in your report, on January 18, 2005, all responsibility for adding and deleting of PRIME contractors was assumed by an IRS PRIME System Access Manager (PSAM). In addition, since February 2005, all new PRIME contractors are instructed during their OL-5081 orientations to provide brief justification statements in the Special Instructions box on the 5081 request screen for all of their applications' requests.

Further, the PRIME Computer Sciences Corporation (CSC) liaison was informed that any OL 5081 application requests received by the PSAM without justification statements would be disapproved. This information was shared with all PRIME contractors. The

direction to provide justification statements for all requests is being formalized in the next update to the Contractor Guide projected for publication in January 2006.

To ensure that all PRIME contractor accesses are granted only to those contractors who have been determined to need a given application or sub-application, a Memorandum of Understanding (MOU) is being drafted and will be coordinated with our Office of Procurement and other impacted officials. Additional information is provided in our narrative for Corrective Action #1.

We have also added a contract clause in the Program Management Plan for 2005, requiring the Contractor to notify the IRS three (3) days in advance of termination, if possible, or within two (2) business days if advance notification is not feasible. Since the IRS PSAM assumed responsibility for managing PRIME contractor access to IRS systems applications and sub-applications, all contractor deletion requests are given the highest priority and the contractors whose names are in the OL-5081 database are promptly marked as "Separated". A contract Modification to the PRIME Contract completely replaced the Security Requirement Clause H.13 in the PRIME Contract and became effective on May 12, 2005. This clause provides that BSMO with the assistance of Mission Assurance and Security Services and CSC, develop an Information Technology Security Plan consistent with the FISMA guidelines which incorporates the IRS/Treasury security requirements. The PRIME will be expected to adopt the plan and promulgate its use throughout its organization.

Your report states that, "*the PRIME contractor added 199 user accounts without any oversight by the IRS during this 1-year period.*" Later in your report you also make an observation that, "as *of May 2005, most of these accounts had been deactivated, but 160 of these contractor employees still had access to IRS systems.*"

We reviewed these accounts. Our review showed that of the 199 users, 128 are included in the 160. However, we concentrated first on the list of 160 contractor employees reported as still having access to IRS systems. Currently, our review shows that none of the 160 contractors identified are on the OL-5081 system erroneously. Only 17 of the160 are still present and all 17 are listed appropriately. The remaining 71 are not currently on the OL-5081 system and we verified that they are not currently performing services for IRS on the PRIME contract. We will continue our research into your findings.

When addressing PRIME contractor's remote access to the IRS network, you acknowledged that the data link between the PRIME contractor's offices and the IRS was properly encrypted and physical security at the PRIME contractor's work site was adequate. We are delighted that the audit identified that security controls in place in these areas were effective.

The official draft report generally reflects the condition of the IRS and we appreciate the audit team incorporating the IRS comments provided on the earlier versions of the draft report. We concur with the three report recommendations which will further assist us in

strengthening controls associated with contractor access to IRS systems and the review of audit trails for contactors. Our detailed response to each report recommendation is in the attachment. If you have any questions, please contact me at (202) 622-8910.

Attachment

Attachment

Management Response to Draft Audit Report - Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved (Audit # 200520002)

RECOMMENDATION #1: The Chief Information Officer, in coordination with the Director, Procurement, should ensure COTRs obtain sufficient documentation from the PRIME contractor to justify access to IRS systems. Before granting access to a contractor employee, the PRIME System Access Manager should obtain acknowledgement from the respective COTR that the access is needed.

CORRECTIVE ACTION TO RECOMMENDATION #1:
We agree with this recommendation. A Memorandum of Understanding (MOU) has been drafted to all PRIME COTR's, PRIME Acquisition Program Managers (APMs), PRIME Program Managers (PMs), and the PSAM outlining the roles and responsibilities of each office involved in the process of ensuring that contractors only gain access to those IRS systems that are needed for them to perform their work assignments.

In addition, a project profile will be created for all PRIME projects with input from the PM's and APM's. The profile will provide a list of all applications needed by the contractors assigned to each project. This information will be used by the PSAM to effectively determine whether or not to approve a contractor's request on the On-Line 5081 system. The draft MOU will be issued to all of the above-listed partners for their review in the month of September 2005. In October 2005, meetings will be scheduled and the profiles will be finalized. A finalized MOU will be signed by all partners prior to 12/31/2005.

IMPLEMENTATION DATE:
January 01, 2006

RESPONSIBLE OFFICIAL:
Deputy Associate Chief Information Officer, Systems Integration

CORRECTIVE ACTION MONITORING PLAN:
Accepted corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and on the Item Tracking, Reporting, and Control System (ITRAC). These corrective actions are monitored on a monthly basis until completion.

COST: .33 SY
Priority: High
Category: Security

1

Attachment

Management Response to Draft Audit Report - Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved (Audit # 200520002)

RECOMMENDATION #2: The Chief Information Officer, in coordination with the Director, Procurement, should require the PRIME System Access Manager to review the active account list quarterly for all applications used by the PRIME contractor to ensure accounts no longer needed are promptly disabled.

CORRECTIVE ACTION TO RECOMMENDATION #2:
We agree with this recommendation. The Director, Procurement will modify the Program Management Office (PMO) task order to require the PRIME contractor to submit a list of terminated employees on a quarterly basis. The PRIME COTRs will use this list to determine which accounts need to be deactivated. A quarterly active account list will be downloaded and sent to the appropriate COTR for review and analysis. Any accounts that are no longer needed will be identified by the COTR, who will report these to the PSAM. The PSAM will then input the deletions in the OL-5081 system. This will also be documented in the Memorandum of Understanding (MOU), which was described in Corrective Action #1.

IMPLEMENTATION DATE:
January 01, 2006

RESPONSIBLE OFFICIAL:
Deputy Associate Chief Information Officer, Systems Integration

CORRECTIVE ACTION MONITORING PLAN:
Accepted corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and on the Item Tracking, Reporting, and Control System (ITRAC). These corrective actions are monitored on a monthly basis until completion.

COST: .10 SY
Priority: High
Category: Security

Attachment

Management Response to Draft Audit Report - Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved (Audit # 200520002)

RECOMMENDATION #3: The Chief, Mission Assurance and Security Services, should ensure audit trail reviews of contractor activity are conducted as prescribed by IRS procedures.

CORRECTIVE ACTION TO RECOMMENDATION #3:
We agree with this recommendation. The PRIME test and development environment has been configured as an extension of the IRS network. Consequently, it has been defined as a unique General Support System, MITS-27 and is included in the IRS Federal Information Security Management Act (FISMA) inventory. All automated data processing operations in this environment are subject to the same operational security practices of any other IRS information technology processing environment. Enterprise wide tools, whether for Operating System level auditing, i.e., Aelita, CM, i.e., Tivoli, LEM Checker, VI-SS Scans, or virus protection and patch management, will be deployed on systems in this environment. Operational security duties for this environment will be performed by Information Technology Security Field Operations consistent with other IRS operating environments.

All systems within the MITS-27 boundary have been placed on a unique network subnet address. Instructions will be sent to administrators of production environment systems directing them to include a review of user access from this subnet as a key component of their standard system auditing activities.

IMPLEMENTATION DATE:
October 15, 2006

RESPONSIBLE OFFICIAL:
Associate Director, Information Technology Security Field Operations, MA&SS (Compliance monitoring component)
Associate Director, FISMA Program Office, MA&SS (policy component)

CORRECTIVE ACTION MONITORING PLAN:
Accepted corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and on the Item Tracking, Reporting, and Control System (ITRAC). These corrective actions are monitored on a monthly basis until completion.