TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure

May 18, 2010

Reference Number: 2010-20-051

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

TAXPAYER DATA USED AT CONTRACTOR FACILITIES MAY BE AT RISK FOR UNAUTHORIZED ACCESS OR DISCLOSURE

Highlights

Final Report issued on May 18, 2010

Highlights of Reference Number: 2010-20-051 to the Internal Revenue Service Chief Technology Officer and Chief, Agency-Wide Shared Services.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) provides its taxpayer data to contractors who store and process the data at their own facilities in support of the IRS' mission of tax administration. The IRS did not have effective processes to identify all contractors with IRS taxpayer data that require annual security reviews by the IRS and did not ensure computer security weaknesses identified at contractor facilities during security reviews have been corrected. As a result, taxpayer data may be at risk for unauthorized access or disclosure.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory requirements to annually review the adequacy and security of IRS information technology. The overall objective of this review was to determine whether the IRS had effective controls in place to ensure IRS taxpayer data are protected at contractor facilities.

WHAT TIGTA FOUND

Current processes were not effective at identifying all contractors who receive IRS taxpayer data and are subject to required security reviews. The Infrastructure Security and Reviews (ISR) office identified contractors that require reviews by asking IRS business organizations to identify their contractors that process, store, or house IRS taxpayer data. However, this process did not identify all contractors who have been provided such data. Without an effective process for identifying the contractors receiving IRS taxpayer data, the IRS cannot ensure that all contractors who receive such data are being reviewed for compliance with security requirements. As a result, the IRS cannot ensure that taxpayer data are protected at contractor facilities.

TIGTA also found that security weaknesses identified by the ISR office team at contractor facilities were not timely corrected. Our review of eight contractors visited by the ISR office during Fiscal Year 2009 found that the ISR office identified security weaknesses at all eight contractor facilities. However, the IRS was unable to provide monitoring documents for seven of the eight contractors. These weaknesses included access control, configuration management control, and system integrity control issues. Without adequate oversight to monitor and confirm that security weaknesses are corrected at contractor facilities, security weaknesses will persist and taxpayer data will remain at risk of unauthorized access and disclosure.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS identify the information system that can serve as the primary source for identifying contractors requiring reviews. The IRS should also ensure that appropriate indicators are captured on each existing contract with a disclosure and privacy impact, validate whether the IRS business organization provided any IRS taxpayer data to these contractors, and provide the appropriate notification and guidance to the responsible IRS business organizations to execute annual security reviews of contractors when required. In addition, the IRS should validate correction of reported security weaknesses and recommend a process for reporting weaknesses that remain unmitigated to increase the accountability of the responsible parties for remediation of security weaknesses.

In their response to the report, IRS management agreed with our recommendations and plans to take appropriate corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 18, 2010

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER
CHIEF, AGENCY-WIDE SHARED SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure (Audit # 200920005)

This report presents the results of our review of determine whether the Internal Revenue Service (IRS) had effective controls in place to ensure IRS taxpayer data are protected at contractor facilities. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2010 Annual Audit Plan and addresses the major management challenge of Security at the IRS and was part of our statutory requirement to annually review the adequacy and security of IRS information technology.

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

Table of Contents

Abbreviations

FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
ISR	Infrastructure Security and Reviews
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones

Background

In its Fiscal Year 2001 summary report to Congress, the Office of Management and Budget identified the security of contractor-provided services as a Government-wide challenge to information technology security. When the Federal Information Security Management Act (FISMA)[1] was enacted a year later, provisions and guidelines were promulgated to ensure the effectiveness of information security controls supporting Federal operations and assets by contractors.

The Internal Revenue Service (IRS) uses contractors to help achieve its mission to administer the nation's Federal tax system. Many of these contractors are provided IRS taxpayer data for use at contractor facilities outside of IRS offices. Others contractors operate information systems at contractor facilities on behalf of the IRS that provide access to the IRS network. Like IRS-managed computer systems, contractors must comply with security control requirements issued by the National Institute of Standards and Technology (NIST) for protecting IRS data. The IRS is ultimately responsible for ensuring security controls at contractor facilities are in place and operating effectively.

Specifically within the IRS, the Infrastructure Security and Reviews (ISR) office of the Modernization and Information Technology Services organization Cybersecurity function is responsible for reviewing controls of contractors who receive IRS taxpayer data for use or operate information systems on behalf of the IRS at contractor facilities to ensure security requirements have been implemented. The ISR office schedules and conducts reviews of these contractors on an annual basis, using the methodology defined in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* and NIST Special Publication 800-53A, *Guide for Assessing Controls in Federal Information Systems*.

This review was performed at the Modernization and Information Technology Services organization Headquarters in New Carrollton, Maryland, and at one contractor facility in Sterling, Virginia, during the period June 2009 through January 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe 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] E-Government Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946.

Results of Review

During Fiscal Years 2008 and 2009, the ISR office visited 12 and 57 contractors, respectively, to evaluate the security of IRS taxpayer information at the contractor facilities. Based on our review of eight contractors[2] visited by the ISR office during Fiscal Year 2009, we found that the ISR office conducted effective contractor reviews in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* for specifying required security controls and NIST Special Publication 800-53A, *Guide for Assessing the Security Controls for Federal Information Systems,* for assessing the security controls' effectiveness. For the 12 contractors reviewed during Fiscal Year 2008, the ISR office identified 133 security weaknesses and for the 57 contractors reviewed during Fiscal Year 2009, the ISR office identified 268 security weaknesses in the same major control areas. These 401 security weaknesses related to all 17 NIST Special Publication 800-53 control families, including contingency planning (39 weaknesses), configuration management (37 weaknesses), risk assessments (32 weaknesses), and access controls (31 weaknesses).

However, the IRS did not have effective processes to identify all contractors with IRS taxpayer data that require annual security reviews by the IRS and did not ensure computer security weaknesses identified at contractor facilities during security reviews are timely corrected. In order to ensure IRS data are secured at all contractor facilities, the IRS needs to improve its current processes and controls to identify all contractors who process, manage, or store IRS taxpayer data at contractor facilities and to ensure timely corrective actions are taken on computer security weaknesses identified at contractor facilities.

The Internal Revenue Service Did Not Have an Effective Process for Identifying All Contractors Who Have Been Provided Taxpayer Data and Require Computer Security Reviews

The ISR office is required to conduct annual security reviews of contractors who possess or have direct access to IRS information or operate information systems on behalf of the IRS at contractor facilities to ensure security requirements have been implemented. The purpose of these security reviews is to ensure contractors are complying with IRS security policies and procedures, and protecting taxpayer information provided to them. To identify contractors who require these onsite security visits, the ISR office submits an enterprise-wide data call request asking all IRS business organizations to identify their contractors that possess or have access to IRS taxpayer data at contractor facilities. Based on the data call results, the ISR office prepares

[2] See Appendix IV for a listing of the eight contractors we reviewed.

an inventory of contractors and schedules reviews based on a set of priorities, including filing season readiness, risk exposure, and the specific type of tax data processed by the contractor.

This process was not effective at identifying all contractors who have been provided IRS taxpayer data. During our audit fieldwork, we identified one contractor who was not on the contractor inventory list used by the ISR office for tracking their inventory of contractors requiring review but should have been included. In addition, the ISR office had identified a contractor who received IRS data but was previously identified as not receiving IRS taxpayer data by an IRS business organization. In Fiscal Year 2009, the ISR office subsequently reviewed both of these contractors.

These two examples highlight the need for improvement in identifying contractors who receive taxpayer data from the IRS. The contractors who were visited and reviewed by the ISR office in Fiscal Years 2008 and 2009 were identified by IRS business organizations responding to the data call. In Fiscal Year 2009, the ISR office also obtained a list of 1,396 procurement requests from an IRS procurement information system used to manage the IRS procurement process. All of these procurement requests contained disclosure and privacy indicators, which informed the IRS contracting office that the contractor would use IRS data at the contractor's facility.[3] However, due to the workload involved, neither the ISR office nor the IRS Procurement organization reviewed these procurement requests to determine whether contractors were, in fact, provided IRS taxpayer data and, therefore, required an annual security review.

While not all of these 1,396 procurement requests may include contractors who process, manage, or store IRS taxpayer data at contractor facilities, we believe the contract data contained in the procurement information system may provide the most definitive, reliable, and complete source for identifying such contractors. However, improvements are needed to the procurement information system in order for the system to readily determine which contractors meet the ISR office criteria for requiring a contractor review. Without an effective process for identifying these contractors, the IRS cannot ensure that all contractors who have been provided IRS taxpayer data are being reviewed for computer security control weaknesses. As a result, the IRS cannot ensure that taxpayer data are protected at all contractor facilities.

Recommendations

Recommendation 1: The Chief, Agency-Wide Shared Services, and the Chief Technology Officer should identify the information system that can serve as the primary source for identifying contractors requiring ISR office security reviews and develop specific indicators

[3] The disclosure and privacy indicator field on the procurement information system corresponds to the question, "Does your requirement involve Sensitive But Unclassified information where Information Technology services are performed at the contractor's site or with the use of the contractor's electronic devices (e.g., laptops, blackberries, text messaging cellular equipment, thumb drives, CDs, etc.)?" If answered yes, disclosure and privacy clauses are included in the contract.

within the information system that effectively identify any contractor receiving and using IRS taxpayer data at the contractor's facility.

> ***Management's Response:*** IRS management agreed with this recommendation. The Chief, Agency-Wide Shared Services, will modify the Personal Identity Verification Background Investigation Process system to identify candidate contracts and contractors who have access to sensitive information. The ISR office will use reports from this system and related information to identify contractor facilities for review.

Recommendation 2: The Director, Procurement, and the Director, Office of Privacy and Information Protection, should ensure the appropriate indicator is captured on each existing contract with a disclosure and privacy impact, validate whether the business organization provided any IRS taxpayer data to these contractors, and provide the appropriate notification and guidance to the responsible IRS business organizations to execute annual security reviews of these contractors when required.

> ***Management's Response:*** IRS management agreed with this recommendation. The Director, Procurement, and the Director, Physical Security and Emergency Preparedness, will track the appropriate indicators and provide the ISR office with contract and contractor information for use in selecting contractor sites for security reviews.

The Internal Revenue Service Did Not Ensure Computer Security Weaknesses Identified at Contractor Facilities Are Timely Corrected

Office of Management and Budget memorandum M-08-21, entitled "Fiscal Year 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," states that FISMA requirements follow agency information into any system which uses it or processes it on behalf of the agency. When the ultimate responsibility and accountability for control of the information continues to reside with the agency, FISMA requirements apply. To the extent that contractors process, store, or house Federal Government information or operate information systems on behalf of the IRS at contractor facilities, the contractor's security controls must be assessed against the same NIST criteria and standards as any Government agency. Further, the agency is responsible for ensuring the contractor corrects weaknesses discovered through self-assessments and independent assessments. Any weaknesses are to be reflected in the agency's Plan of Action and Milestones (POA&M).[4]

IRS policy requires business and system owners to ensure that all acquisitions of goods or services provide for information security, personnel security, and physical security, which includes the security of any IRS data at contractor facilities. Further, IRS policy requires the

[4] A POA&M document, also referred to as a corrective action plan, is a tool that assists agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Contracting Officer's Technical Representative to ensure that contractors comply with IRS security policies and pursue appropriate action for noncompliance. As a means to determine whether contractors are complying with IRS security policies, the ISR office is responsible for evaluating the security of IRS taxpayer data at contractor facilities.

After the ISR office completes a contractor security review, the ISR office presents the results to the Contracting Officer's Technical Representative in a Security Assessment Report, which includes the details of the security weaknesses identified at the contractor's facilities. The ISR office instructs the Contracting Officer's Technical Representative to coordinate with the Designated Approving Authority or the Security Program Management Office to identify corrective actions and planned implementation dates for resolving the weaknesses. The ISR office further instructs the Security Program Management Office to provide oversight, in coordination with the Contracting Officer's Technical Representative, to ensure remediation of each weakness identified, including developing and maintaining a corresponding item on the POA&M.

However, the IRS was not consistently developing the POA&Ms for security weaknesses identified by the ISR office. In our judgmental sample of eight contractors visited by the ISR office during Fiscal Year 2009, all eight contractors' facilities had security weaknesses identified by the ISR office. We requested copies of the POA&Ms for tracking these security weaknesses. The IRS was unable to provide the POA&Ms developed as a result of the ISR office reviews for seven of the eight contractors. During the course of our audit, the POA&Ms were developed for four of the seven contractors in our sample that were not provided when we requested them.

When asked why the POA&Ms were not completed for the seven contractors, the IRS stated it did not create and monitor ISR office findings in the POA&Ms for systems that it did not consider as FISMA reportable systems[5] or did not believe the contractors were subject to FISMA requirements. We disagree with this reasoning. However, while there might be confusion over what is or is not FISMA reportable, we believe the approach for tracking and monitoring security weaknesses should apply regardless of whether or not FISMA applies to the contractor since the weaknesses pertain to the protection of IRS taxpayer data. When security weaknesses are not tracked and monitored, the IRS has no assurance that an official within the IRS is taking responsibility for monitoring the security weaknesses reported by the ISR office and ensuring security weaknesses are timely addressed.

To illustrate the importance of monitoring security weaknesses at contractors' facilities, the ISR office identified 6 repeat security weaknesses at contractor facilities during its Fiscal Year 2008 reviews and 24 repeat security weaknesses during its Fiscal Year 2009 reviews that were not corrected since the prior fiscal years' ISR office reviews. These security weaknesses included

[5] Systems subject to FISMA contractor reviews include contractors with privileged access to IRS data and/or contractors that manage a process or system at a contractor-owned or operated facility on behalf of the IRS.

access control, configuration management control, and system integrity control issues. For example, the ISR office found that some contractors:

- Had system security settings not set to the most restrictive mode.
- Lacked policies on how to handle sensitive information.
- Had systems that were less than 90 percent compliant with IRS security policies based on automated scans of system settings.

The eight contracts that we reviewed generally required the contractors to adhere to IRS security policies and procedures. Without adequate oversight to monitor and confirm that security weaknesses are corrected at contractor facilities, security weaknesses will persist and IRS data will remain at risk for unauthorized access and disclosure.

Recommendations

Recommendation 3: The Associate Chief Information Officer, Cybersecurity, should validate correction of ISR office reported security weaknesses and recommend a process for reporting weaknesses that remain unmitigated to increase the accountability of the responsible parties for remediation of security weaknesses.

> ***Management's Response:*** IRS management agreed with this recommendation. The ISR office will establish a plan for requesting status updates on the POA&Ms from the responsible parties, validate corrected security weaknesses, and inform the responsible parties of uncorrected weaknesses quarterly.

Recommendation 4: The Director, Procurement, and the Associate Chief Information Officer, Cybersecurity, should work together to ensure contractor accountability that security weaknesses are addressed in a timely manner. Using validation results from Recommendation 3, the Procurement organization, working with the Cybersecurity organization, will take appropriate action and employ all rights and remedies available to the Government if and when contractors do not comply with IRS security policies.

> ***Management's Response:*** IRS management agreed with this recommendation. Based on validation results from the ISR office, the Director, Procurement, and the Associate Chief Information Officer, Cybersecurity, will determine the appropriate action and employ all rights and remedies available to the Government if and when contractors do not comply with IRS security policies.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS had effective controls in place to ensure IRS taxpayer data are protected at contractor facilities. In order to accomplish our objective, we:

I. Determined whether IRS contractor reviews were adequate to validate contractor compliance with IRS security policies.

A. Selected a judgmental sample of 8 contractors that process, manage, or store Federal taxpayer information or operate information systems on behalf of the IRS at non-IRS locations from an IRS list of 57 contractors that required an annual security review during Fiscal Year 2009. This list was the result of the data call that the IRS makes to its business organizations annually to identify contractors to schedule for a security review. We selected a judgmental sample because we did not plan to project the results.

B. Obtained and reviewed contracts for the selected contractors and determined whether each was adequate to hold contractors accountable for implementing IRS security policies.

C. Obtained and reviewed contractor review plans and results prepared by the IRS for the selected contractors and evaluated them for adequacy.

D. Determined whether any weaknesses identified were being tracked in a POA&M and whether progress was being made to correct the deficiencies.

II. Determined whether key information system controls were in place and operating effectively to limit access to only authorized users at one contractor facility at a non-IRS location. We reviewed the following types of controls:

A. Access.

B. Identification and Authentication.

C. Audit and Accountability.

D. Risk Assessment.

E. System and Information Integrity.

III. Evaluated the process for identifying contractors provided IRS taxpayer data for use at offsite locations.

A. Reviewed the data call method used by the IRS to identify contractors requiring an annual security review.

B. Reviewed procurement request data from an IRS procurement system and determined whether the IRS procurement system could be used to automate identification of contractors requiring an annual security review. To assess the reliability of the procurement request data, we interviewed knowledgeable agency officials about the data and reviewed relevant documentation. We determined that the data were sufficiently reliable for the purposes of this report.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: the IRS' policies, procedures, and practices for ensuring IRS data are secured at offsite contractor locations. We evaluated these controls by reviewing contracts, security control testing results, and related documentation and consulting with IRS and contractor personnel.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Lead Auditor
Richard Borst, Senior Auditor
Michelle Griffin, 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, Privacy, Information Protection, and Data Security OS:P
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Director, Privacy and Information Protection OS:P:PIP
Director, Procurement OS:A:P
Director, Cybersecurity Program and Policies OS:CTO:C:PP
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Chief Technology Officer OS:CTO
    Chief, Agency-Wide Shared Services OS:A

Appendix IV

Listing of Contractors Selected for Review

From an IRS list of contractors that required contractor reviews, we selected a judgmental sample of eight contractors who process, manage, or store Federal taxpayer information or operate information systems on behalf of the IRS at non-IRS locations. We reviewed the contracts, the methods of security control testing, the Security Assessment Reports provided by the IRS Infrastructure Security and Reviews team, and the processes to resolve weaknesses.

	Contractor	Description of System	Location	Business Organization
1	Northrop Grumman Information Technology	Service Center Recognition Image Processing System	Reston, Virginia	Wage and Investment
2	Accenture/Affina/Qwest	Health Coverage Tax Credit Program	Iowa, Virginia, and Texas	Wage and Investment
3	AT&T	Enterprise Remote Access Project	Oakton, Virginia	Modernization and Information Technology Services
4	Accenture	IRS.gov Public User Portal	Reston, Virginia	Modernization and Information Technology Services
5	IBM/Quest	Registered User Portal	Sterling, Virginia, and Chicago, Illinois	Modernization and Information Technology Services
6	Computer Sciences Corporation	Development, Integration, and Testing Environment	Lanham, Maryland	Modernization and Information Technology Services
7	CRA International	The contractor is supplied with Sensitive But Unclassified data in order to perform appraisal or actuarial work – valuation of minority stock interests.	Chicago, Illinois	Small Business/ Self-Employed
8	Pacific Consulting Group	Data and market research	Palo Alto, California	Wage and Investment

Appendix V

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

RECEIVED
APR 12 2010
BY: DAS

April 12, 2010

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure (Audit #200920005) (i-trak #2010-73426)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate your report recognizing that the Internal Revenue Service (IRS) conducted effective contractor security reviews in accordance with standards for security controls on Federal information systems. The purpose of these security reviews is to ensure contractors are complying with IRS security policies and procedures, and protecting taxpayer information provided to them.

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

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

Attachment

Attachment

Draft Audit Report –Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure (Audit # 200920005) (i-trak #2010-73426)

RECOMMENDATION #1: The Chief, Agency-Wide Shared Services, and the Chief Technology Officer should identify the information system that can serve as the primary source for identifying contractors requiring ISR office security reviews, and develop specific indicators within the information system that effectively identify any contractor receiving and using IRS taxpayer data at the contractor's facility.

CORRECTIVE ACTION #1: Agency-Wide Shared Services (AWSS) will modify the Personal Identity Verification (PIV) Background Investigation Process (PBIP) system to identify candidate contracts and contractors who have access to Sensitive But Unclassified (SBU) information at a contractor's facility. MITS Cybersecurity will use PBIP reports, along with information from security plans provided by COTRs, to identify contractor facilities to be reviewed based on a valid statistical sample.

IMPLEMENTATION DATE: October 1, 2010

RESPONSIBLE OFFICIAL: Director, Physical Security and Emergency Preparedness (AWSS) and Associate Chief Information Officer, Cybersecurity (MITS)

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 Director, Procurement, and the Director, Office of Privacy and Information Protection, should ensure the appropriate indicator is captured on each existing contract with a disclosure and privacy impact, validate whether the business organization provided any IRS taxpayer data to these contractors, and provide the appropriate notification and guidance to the responsible IRS business organizations to execute annual security review of these contractors when required.

CORRECTIVE ACTION #2: The Director, Procurement, will continue to provide the existing indicators in the web Request Tracking System (webRTS) to identify when privacy and disclosure clauses are needed in contracts, and will provide that data to MITS Cybersecurity. The Director, Physical Security and Emergency Preparedness, will track contractor employees who are to be given access to Sensitive But Unclassified (SBU) data in the Personal Identity Verification (PIV) Background Investigation Process (PBIP) system, and provide that data to Cybersecurity. Using this data, Cybersecurity, based on a valid statistical sample will identify candidates for annual security reviews and execute annual security reviews of these contractors when required.

IMPLEMENTATION DATE: October 1, 2010

Attachment

Draft Audit Report –Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure (Audit # 200920005) (i-trak #2010-73426)

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity (MITS) and the Director, Physical Security & Emergency Preparedness (AWSS)

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

RECOMMENDATION #3: The Associate Chief Information Officer, Cybersecurity, should validate correction of ISR office reported security weaknesses and recommend a process for reporting weaknesses that remain unmitigated to increase the accountability of the responsible parties for remediation of security weaknesses.

CORRECTIVE ACTION #3: Cybersecurity's Infrastructure Security and Review (ISR) Office will establish a plan that delineates sending out a request for status updates on Plans of Action & Milestones (POA&Ms) from the responsible Business Unit. As appropriate, ISR will validate the correction of findings in the POA&M during the POA&M continuous monitoring process or during follow-up security reviews.

In addition, ISR will forward a copy of uncorrected weaknesses to the appropriate business unit executive each quarter to ensure that the responsible parties are made aware of the need to remediate weaknesses.

IMPLEMENTATION DATE: December 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity (MITS)

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 Director, Procurement, and the Associate Chief Information Officer, Cybersecurity, should work together to ensure contractor accountability that security weaknesses are addressed in a timely manner. Using validation results from recommendation #3, the office of Procurement, working with the Cybersecurity organization, will take appropriate action and employ all rights and remedies available to the Government if and when contractors do not comply with IRS security policy.

CORRECTIVE ACTION #4: Based on validation results from Cybersecurity's Infrastructure Security and Review (ISR) Office, the Director, Procurement, and the Associate Chief Information Officer, Cybersecurity, will determine the appropriate action and employ all rights and remedies available to the Government if and when contractors do not comply with IRS security policy.

Attachment

Draft Audit Report –Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure (Audit # 200920005) (i-trak #2010-73426)

IMPLEMENTATION DATE: Implemented April 1, 2010

RESPONSIBLE OFFICIALS: Director, Procurement (AWSS) and Associate Chief Information Officer, Cybersecurity (MITS)

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.