



*Insufficient Attention Has Been Given to
Ensure States Protect Taxpayer Information*

August 31, 2007

Reference Number: 2007-20-134

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-927-7037

Email Address | Bonnie.Heald@tigta.treas.gov

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



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

August 31, 2007

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – Insufficient Attention Has Been Given to Ensure
States Protect Taxpayer Information (Audit # 200720025)

This report presents the results of our followup review to determine whether Federal tax information provided to third parties (in this case, State agencies) is protected from unauthorized access, use, and disclosure. We evaluated the effectiveness of the Internal Revenue Service's (IRS) actions to correct computer security weaknesses at State agencies that we had reported in September 2005.¹ This audit is part of the statutory audit coverage under our Information Systems Programs unit and is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2007 Annual Audit Plan.

Impact on the Taxpayer

The IRS provides taxpayers' personal and financial data to agencies in all 50 States to assist them in carrying out their own tax administration responsibilities. The IRS Safeguard Review program is responsible for ensuring the States provide adequate security over that information to prevent unauthorized disclosures that could be used for identity theft and other fraudulent activities. Without an effective Safeguard Review program, the IRS has little assurance the information provided to the States is adequately protected and funds are prudently spent on contractor support.

¹ *Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 2005).



Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information

Synopsis

As a result of our 2005 review of the Safeguard Review program, the IRS agreed to:

- Revise guidance to States found in *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (Publication 1075) for conducting their security self-assessments to incorporate the recommended security controls described in the National Institute of Standards and Technology (NIST)² guidance required for all Federal Government agencies.
- Assign more staffing to the Mission Assurance and Security Services organization's Safeguard Review program to provide adequate oversight to the States.
- Improve the scope of IRS Safeguard Reviews by incorporating appropriate NIST guidance into the computer security Safeguard Review process.
- Use Plans of Action and Milestones to better monitor recommended corrective actions for weaknesses identified.

Since our 2005 review, the IRS has revised guidance to the States to incorporate the recommended security controls described by the NIST. We anticipate the guidance will assist the State agencies in performing more complete security assessments of their computer systems.

To improve the Safeguard Reviews, the IRS awarded a 5-year contract to Booz Allen Hamilton to supplement the Safeguards Review staff in conducting more reviews. However, the other corrective actions to our prior report have not yet been taken or have not been effective to improve the scope of the Safeguard Reviews and to monitor corrective actions. Also, the IRS is not timely reporting the results of its Safeguard Reviews to the States. We attribute these weaknesses to the lack of management oversight.

During the course of our review, we became very concerned at the lack of management attention being directed to the Safeguard Review program. As a result, we expanded our review to assess the administration of the contract with Booz Allen Hamilton. Controls over the contract were insufficient to ensure the Federal Government receives the services for which it contracted, on time, and in accordance with specifications. Additional oversight for the contract is needed so the IRS can ensure it is prudently spending the \$1.4 million designated annually for the Safeguard Review program. Due to the poor contract oversight provided by the IRS, we requested additional documentation from the contractor. We will report our assessment of the contractor documentation in a future Office of Audit document.

² The NIST is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.



Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information

In July 2007, the IRS Mission Assurance and Security Services organization was realigned and the responsibilities for the Safeguard Review program were transferred to the Small Business/Self-Employed Division. While the Small Business/Self-Employed Division has taken the responsibility of responding to the recommendations in this report, we are issuing the report to the Chief, Mission Assurance and Security Services, at his request.

Recommendations

We recommended the Chief, Mission Assurance and Security Services, provide management oversight for the Safeguard Review program sufficient to ensure test plans used during Safeguard Reviews are revised and consistent with IRS guidance, the corrective action to our prior report is reopened to ensure the development and implementation of a Plan of Action and Milestones process, Safeguard Review results are provided timely to the States, task orders³ clearly define deliverables for the contractor, and contractor billings are monitored to ensure funds are prudently spent.

Response

IRS management agreed with all of our recommendations. The Director, Communications, Liaison and Disclosure, Small Business/Self-Employed Division, will initiate additional changes to the recently revised Publication 1075 to incorporate guidance for executing test plans used in Safeguard Reviews. The corrective action corresponding to the followup and monitoring of corrective actions will be reopened, and a Plan of Action and Milestones process will be developed. Also, Safeguard Review results will be provided to the States within 30 calendar days of the review, but not later than 45 calendar days after the closing conference, in accordance with IRS procedures. A monthly monitoring plan will be developed to track reports and ensure followup actions have been taken on a timely basis.

The Small Business/Self-Employed Division has assigned a task representative to work with the Contracting Officer's Technical Representative and manage all aspects of contract support. The task representative will oversee the contractors' work and perform monthly contract reviews to ensure the accuracy of the invoices and that work authorized is completed in accordance with the work requests. Work requests will be signed by the task representative, the Contracting Officer's Technical Representative, and the contractor manager prior to starting work and upon completion of the task. In addition, a project manager has been added to the Safeguards Review staff to provide guidance, oversight, and monitoring of the program contract. Management's complete response to the draft report is included as Appendix IV.

³ A task order is an order for services placed against an established contract.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

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.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Table of Contents

BackgroundPage 1

Results of ReviewPage 3

 Actions Have Been Taken to Improve the Scope of State Safeguard
 Activity ReportsPage 3

 Adequate Actions Have Not Been Taken to Improve Internal Revenue
 Service Safeguard Reviews.....Page 3

Recommendation 1:.....Page 5

Recommendations 2 and 3:Page 6

 The Office of Privacy and Information Protection Is Not Adequately
 Monitoring Contracting ActionsPage 6

Recommendation 4:.....Page 7

Recommendation 5:.....Page 8

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 9

 Appendix II – Major Contributors to This ReportPage 11

 Appendix III – Report Distribution ListPage 12

 Appendix IV – Management’s Response to the Draft ReportPage 13



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Abbreviations

IRS

Internal Revenue Service

NIST

National Institute of Standards and Technology



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Background

Internal Revenue Code Section 6103 authorizes the Internal Revenue Service (IRS) to disclose Federal tax information to various State and Federal Government agencies. In 2005, the IRS provided taxpayer information to all 50 States, whose tax agencies can use the information to identify nonfilers of State tax returns, determine discrepancies in the reporting of income, locate delinquent taxpayers, and determine whether IRS adjustments have State tax consequences.

The Safeguard Review program should ensure State agencies receiving Federal tax information maintain adequate safeguards to protect the data.

As a condition for receiving Federal tax information, State tax agencies must have physical and computer system safeguards designed to prevent unauthorized accesses and use of this information. Before a State tax agency receives Federal tax information, it must submit a Safeguard Procedures Report to the IRS for approval. The Safeguard Procedures Report describes how the State will protect and safeguard the tax information. In addition, States are required to annually file Safeguard Activity Reports to describe any changes to their safeguard procedures, advise the IRS of future actions that will affect safeguard procedures, and certify they are protecting the data.

The Safeguard Review program within the Office of Privacy and Information Protection in the Mission Assurance and Security Services organization should ensure State agencies receiving Federal tax information maintain adequate safeguards to protect the data. It is responsible for conducting Safeguard Reviews of each State agency receiving Federal tax information at least once every 3 years. The Safeguard Reviews should evaluate the State agencies' compliance with security procedures to ensure the information is adequately protected.

In 2003, we reported¹ that Federal tax information was at risk while in the possession of State tax agencies. In 2005, we followed up² on the 2003 report and determined these problems persisted. We also noted that State agencies' Safeguard Activity Reports were not effective because they did not adequately test security controls. In addition, IRS Safeguard Reviews were not effective because adequate staffing had not been assigned to conduct a sufficient number of reviews, the scope of reviews was insufficient, and the IRS did not have an adequate process to track corrective actions on weaknesses identified.

¹ *Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk* (Reference Number 2003-20-064, dated February 2003).

² *Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 2005).



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

During the review, the Mission Assurance and Security Services organization was realigned. The responsibility for the Safeguard Review program was transferred to the Small Business/Self-Employed Division in July 2007.

To follow up on the IRS' actions to correct these conditions, we conducted this review at the Office of the Chief, Mission Assurance and Security Services, in Washington, D.C., during the period December 2006 through May 2007. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Results of Review

Actions Have Been Taken to Improve the Scope of State Safeguard Activity Reports

In 2005, we reported significant control weaknesses at the States we reviewed and determined the States were not conducting adequate self-assessments of their security controls. We recommended the IRS revise *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (Publication 1075) to incorporate the security controls described in the National Institute of Standards and Technology (NIST)³ *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53). This NIST document must be followed by Federal Government agencies, and the NIST encourages its use by other organizations.

In response to our report, the IRS agreed to revise Publication 1075 and issued the revision in February 2007. We compared Publication 1075 to NIST Special Publication 800-53 and determined it did address the necessary security controls. We anticipate the revised Publication 1075 will provide guidance for the State agencies to perform more complete security assessments of their computer systems.

Adequate Actions Have Not Been Taken to Improve Internal Revenue Service Safeguard Reviews

In 2005, we reported that the IRS Safeguard Reviews were inadequate and incomplete. We recommended and the IRS agreed to take the following actions to improve its Safeguard Reviews of the States:

- Assign more staffing to the Mission Assurance and Security Services organization's Safeguard Review program to provide adequate oversight to the States.
- Improve the scope of IRS Safeguard Reviews by incorporating appropriate NIST Special Publication 800-53 security controls into the computer security Safeguard Review process.
- Use Plans of Action and Milestones to better monitor recommended corrective actions for weaknesses identified.

³ The NIST is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

In response to our recommendation to assign additional staffing, the Office of Privacy and Information Protection awarded a 5-year contract in May 2006 to Booz Allen Hamilton to supplement the Safeguards Review staff and help meet its requirements to conduct the appropriate number of Safeguard Reviews each year. During Fiscal Years 2005 and 2006, the IRS, with assistance from the contractor, conducted 152 Safeguard Reviews of State agencies receiving Federal tax information. The additional resources provided by the contractor have had a positive impact on the number of Safeguard Reviews conducted of State agencies.

The IRS has not taken sufficient actions in response to our recommendation to improve the scope of the Safeguard Reviews. Language included in the contract with Booz Allen Hamilton required the contractor to update Safeguard Review test plans and customize them as needed, depending on the operating systems used by the States. However, the contract does not define how the test plans are to be updated, specifically that they should incorporate the NIST Special Publication 800-53 security controls.

Additionally, the number of test plans to be updated or customized is not defined in the contract. While the contractor has revised test plans for six operating systems to include many of the control areas described in NIST Special Publication 800-53, these test plans are still in draft form and are currently not being used. When asked, IRS management stated they did not know when the contractor was scheduled to complete the revision of these 6 and the remaining 16 test plans or when they would be available for use.

The Safeguard Reviews conducted in Fiscal Years 2006 and 2007 followed the test plans used prior to our 2005 audit. These plans did not adequately address tests for some of the controls included in NIST Special Publication 800-53, such as incident response, risk assessments, and contingency planning. Until these documents are updated and followed by contractors conducting the tests, the IRS will not be assured that States are adequately protecting Federal tax information. The corrective actions associated with our recommendation are due to be completed in October 2008.

In response to our recommendation to use Plans of Action and Milestones, the IRS agreed to implement this process by August 2006. In May 2006, the IRS formally closed the recommendation by stating it had implemented the process. During this review, we determined the IRS has not implemented the use of Plans of Action and Milestones and still does not have a process to monitor security weaknesses identified during Safeguard Reviews. Management in the Office of Privacy and Information Protection stated that an automated Plan of Action and Milestones tool is under development by the contractor, but a delivery date was unknown. When asked, the IRS could provide no explanation as to why it had stated its actions to implement the Plans of Action and Milestones process were completed in May 2006.

Without a formalized process, the States are not held accountable for addressing weaknesses found during their tests and the tests conducted by the Mission Assurance and Security Services



Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information

organization. As a result, the IRS cannot be certain that deficiencies found during Safeguard Reviews are timely and efficiently corrected.

Also, the IRS was not timely reporting the results of its Safeguard Reviews to the States. IRS procedures state Safeguard Review reports should be provided to State agencies within 30 calendar days of the review but not later than 45 calendar days after the closing conference.

For 2006 and 2007, we reviewed all 18 Safeguard Review reports issued to State tax agencies and determined these reports were issued an average of 81 calendar days after completion of onsite reviews. With these delays, security weaknesses identified in Safeguard Reviews may go unaddressed for months, increasing the risk that Federal tax information may be inappropriately accessed or used.

Security weaknesses at the States could provide opportunities for hackers, disgruntled employees, and contractors to access Federal tax information for unauthorized use and identity theft purposes. Without an adequate Safeguard Review program, the IRS has little assurance that States are maintaining adequate controls over Federal tax information.

We attribute the inability to improve the IRS Safeguard Review program to a lack of management attention and oversight. While sufficient funding has been provided to increase the number of reviews conducted, little emphasis has been placed on enhancing the scope of the reviews, ensuring actions to improve security vulnerabilities are monitored, and ensuring review results are reported timely. Also, IRS employees and contractors were being provided little direction, their work was not being adequately monitored, and desk procedures were not available.

Recommendations

To address these weaknesses, the Chief, Mission Assurance and Security Services, should provide management oversight for the Safeguard Review program sufficient to ensure:

Recommendation 1: The test plans used during Safeguard Reviews are revised and consistent with the guidance found in IRS Publication 1075.

Management's Response: Management agreed with the recommendation. At this time, the contractor has revised most of the Safeguard Computer Security Evaluation Matrices, making them consistent with the requirements of NIST Special Publication 800-53. Communications are pending to all agencies advising them that they will be held to the new standards effective October 1, 2007. The Director, Communications, Liaison and Disclosure, Small Business/Self-Employed Division, will initiate additional changes to the guidance provided in the recently revised Publication 1075 (dated February 2007) to stagger reporting deadlines for Safeguard Activity Reports, as well as incorporate additional guidance for executing test plans used in Safeguard Reviews.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Recommendation 2: The corrective action corresponding to the followup and monitoring of corrective actions is reopened, and a Plan of Action and Milestones process is developed and implemented.

Management's Response: Management agreed with the recommendation. The corrective action corresponding to the followup and monitoring of corrective actions will be reopened and a Plan of Action and Milestones process will be developed. The majority of development work on the newly designed automated Plan of Action and Milestones monitoring tool has been completed by the contractor.

Recommendation 3: The Safeguard Review results are provided timely to the States.

Management's Response: Management agreed with the recommendation. Safeguard Review results will be provided to the States within 30 calendar days of the review, but not later than 45 calendar days after the closing conference, in accordance with IRS procedures. Management will develop a monthly monitoring plan to track reports and ensure followup actions have been taken on a timely basis.

The Office of Privacy and Information Protection Is Not Adequately Monitoring Contracting Actions

During the course of our review, we became very concerned at the lack of management attention being directed to the Safeguard Review program. As a result, we expanded our review to assess the administration of the contract with Booz Allen Hamilton. IRS procedures state the purpose of contract administration is to ensure the Federal Government receives the services for which it contracted, on time, and in accordance with specifications.

The IRS has budgeted \$1.4 million annually for contractor support of the Safeguard Review program. However, the Office of Privacy and Information Protection is not providing sufficient oversight for the use of these funds and the contractor's actions. Specifically:

- In January 2007, task orders⁴ for Safeguard Review site visits performed as far back as June 2006 were signed after the fact by the Mission Assurance and Security Services organization and approved by the Contracting Officer's Technical Representative. We were advised that the contractor, not the IRS, requested the task orders.
- The task orders described above listed "TBD" (To Be Determined) for the number of estimated hours needed to establish and manage a Program Office to administer the contract and to perform Safeguard Reviews.
- Three of the eight contractor payment vouchers were not authorized in writing by Mission Assurance and Security Services organization management.

⁴ A task order is an order for services placed against an established contract.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

- The IRS does not have a process in place to collect data needed to perform a validation of the hours billed by the contractor. Without an effective process to collect such data, the IRS is forced to rely on data the contractor provides. The IRS has received monthly reports from the contractor detailing the number of hours charged to each task order. However, these reports do not specify how many hours were charged to specific tasks, such as a site visit or revision of test plans.
- Contract language is vague regarding deliverables expected by the IRS. The only deliverable described in the contract is the Safeguard Review reports. Consequently, there is no expectation regarding the development and maintenance of workpapers supporting the work performed during a Safeguard Review. Our examination of the workpaper files for reviews conducted in 2006 and 2007 determined the files were incomplete and disorganized. Files for 9 of the 28 reviews we attempted to find were missing, and files for 10 other reviews were missing significant documentation such as review plans, minutes from opening and closing conferences for site reviews, and the most recent Safeguard Activity Reports from the State agency. As a result, the IRS acknowledged it had no way to gauge the adequacy of work performed by the contractor.

Essentially, the IRS is allowing the contractor to dictate the terms of the contract and to determine the amount of funds spent. When asked how oversight is provided to the contractor, IRS management responded that the contractor is trusted and its employees are professionals.

Without adequate oversight for contracting actions, the IRS cannot ensure it is prudently spending the \$1.4 million designated for the Safeguard Review program. Due to the poor contract oversight provided by the IRS, we requested additional documentation from the contractor and are continuing to review that documentation. We will report our assessment of the contractor documentation in a future Office of Audit document.

Recommendations

To address these weaknesses, the Chief, Mission Assurance and Security Services, should provide executive and management oversight for the Safeguard Review program sufficient to ensure:

Recommendation 4: Task orders clearly define the staff hours needed per task and the contractor deliverables for the remaining years of the Safeguard Review program contract.

Management's Response: Management agreed with the recommendation. The Small Business/Self-Employed Division has assigned a task representative to work with the Contracting Officer's Technical Representative and manage all aspects of contract support. This task representative will ensure work requests are written for each task area and clearly define 1) the description of the work to be performed in accordance with the statement of work; 2) skill categories and estimated hours per category; 3) required



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

products, due dates, and specific acceptance criteria; 4) performance site; and 5) any additional Federal Government-furnished equipment the contractor may need to complete the task. Work requests will be signed by the task representative, the Contracting Officer's Technical Representative, and the contractor manager prior to starting work and upon completion of the task. Six key work requests have been identified and will be focused on through December 31, 2007. In addition, a project manager has been added to the Safeguards Review staff to provide guidance, oversight, and monitoring of the program contract.

Recommendation 5: Contractor billings are monitored, and contract hours allocated by task are validated to ensure funds are prudently spent.

Management's Response: Management agreed with the recommendation. The Small Business/Self-Employed Division will ensure contractors report hours charged to the contract by task area. Management will ensure a work request is in place for each task area. The assigned dedicated task representative will oversee the contractor's work and perform monthly contract reviews to ensure the accuracy of the invoices and that work authorized is completed in accordance with the work requests. During the contract review, the task representative will review the following contractor-prepared reports prior to their review and approval by the Contracting Officer's Technical Representative: 1) Monthly Status Reports that document work performed and labor hours spent by task area, 2) work requests, and 3) invoices. Issues, if any, will be elevated to the Contracting Officer's Technical Representative to be addressed with the contractor.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether Federal tax information provided to third parties (in this case, State agencies) is protected from unauthorized access, use, and disclosure. To accomplish this objective, we conducted followup tests to evaluate the effectiveness of the IRS' actions to correct computer security weaknesses at State agencies we had reported in September 2005.¹ Specifically, we:

- I. Assessed the adequacy of the IRS Safeguard Review process.
 - A. Reviewed documentation to determine the adequacy of the scope of IRS Safeguard Reviews conducted in Fiscal Years 2006 and 2007 at State tax agencies.
 1. Determined whether *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (IRS Publication 1075) had been revised to incorporate the recommended security controls described in NIST² *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53).
 2. Reviewed all Safeguard Review Reports issued to State tax agencies during Fiscal Years 2006 and 2007 to determine adequacy of the scope of review.
 3. Reviewed all available Safeguard Review files for reviews conducted at State tax agencies in Fiscal Years 2006 and 2007 to determine adequacy of supporting documentation.
 4. Reviewed the test plans developed by contractor Booz Allen Hamilton and used in the Safeguard Reviews to determine whether the plans include the required security controls for a moderate risk control baseline listed in NIST Special Publication 800-53.
 5. Determined whether adequate oversight was provided to the Booz Allen Hamilton contract employees while they developed the revised test plans.
 6. Determined whether the States submitted self-assessments to the IRS and whether these assessments were used in determining/customizing the scope of the Safeguard Reviews.

¹ *Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 2005).

² The NIST is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

- B. Reviewed documentation to determine whether the IRS is providing timely results of the Safeguard Reviews to the State agencies.
 - C. Reviewed documentation to determine whether the process developed in May 2006 for implementing a Plan of Action and Milestones³ to manage recommended corrective actions has been implemented.
- II. Reviewed contract and process documentation to determine whether the Safeguard Review process has sufficient resources to complete the required number of Reviews.
- A. Reviewed contract documentation, including task orders,⁴ for Safeguard Reviews performed by Booz Allen Hamilton employees to determine whether:
 - 1. An adequate number of staff resources with appropriate technical expertise were detailed in contract language.
 - 2. The actual funding for both the IRS and the contractor staffs have been increased appropriately.
 - B. Determined whether the schedule in place to accomplish these Reviews was consistent with the staffing resources available.
 - C. Determined whether the Reviews of State agencies are performed at least once every 3 years, as required by Internal Revenue Code Section 6103.
- III. Determined whether IRS management oversight for the Booz Allen Hamilton contract was adequate.
- A. For the Fiscal Year 2007 Safeguard Reviews, determined the staff hours by skill/labor category (such as Senior Information Technology Specialist, Junior Information Technology Specialist) planned for Booz Allen Hamilton staff support.
 - B. Determined the procedures in place for the IRS Office of Privacy and Information Protection to evaluate the accuracy of the staff hours billed monthly by Booz Allen Hamilton.
 - C. Obtained the monthly billing vouchers submitted by Booz Allen Hamilton and reviewed to ensure appropriate approvals were obtained.
 - D. For the Fiscal Year 2007 schedule, determined whether Booz Allen Hamilton monthly billing vouchers reconciled with the number of Booz Allen Hamilton staff hours provided during fieldwork.

³ The NIST defines a Plan of Action and Milestones as a plan developed to prioritize identified weaknesses and assign dates for remediation.

⁴ A task order is an order for services placed against an established contract.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Marybeth H. Schumann, Audit Manager
Myron L. Gulley, Lead Auditor
Richard T. Borst, Senior Auditor
Abraham B. Millado, Senior Auditor
Thomas P. Nacinovich, Senior Auditor
Joan M. Raniolo, Senior Auditor
William Simmons, Senior Auditor
Esther M. Wilson, Senior Auditor



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Operations Support OS
Commissioner, Small Business/Self-Employed Division SE:S
Chief Information Officer OS:CIO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
 Commissioner, Small Business/Self-Employed SE:S
 Chief Information Officer OS:CIO



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Appendix IV

Management's Response to the Draft Report



COMMISSIONER
SMALL BUSINESS/SELF-EMPLOYED DIVISION

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

RECEIVED
AUG - 8 2007

August 8, 2007

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kathy K. Petronchak *Kathy K. Petronchak*
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – Insufficient Attention Has Been Given to
Ensure States Protect Taxpayer Information (Audit # 200720025)

We have reviewed your draft report, "Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information," and agree with the recommendations.

As stated in your report, at the time of your review the Office of Safeguards was within the Mission Assurance and Security Services organization. To provide more focused oversight, effective July 8th the office was realigned to the Small Business/Self Employed (SB/SE) Division's Communications, Liaison and Disclosure (CLD) organization. SB/SE CLD is responsible for the Service's Disclosure and Fed/State programs, both closely related to Safeguards Review, and the realignment will strengthen the IRS's overall safeguards program.

We are pleased to inform you we have already initiated several actions to address your recommendations, including:

- Discussions with the contractor to strengthen management controls, oversight and monitoring as well as revise work orders
- Selection of one additional Disclosure Enforcement Specialist (DES), with the selection of three more DES positions pending interviews
- Creation of a DES desk guide, providing detailed review steps to improve consistency and uniformity of safeguard reviews and reports
- Addition of a Project Manager position to provide oversight, guidance and monitoring of the existing contract
- Procurement of a second contractor to conduct an organizational assessment of the Safeguards Program and to shadow the IRS/BAH team in a series of safeguard reviews for physical and computer security

We recognize the importance of assuring that governmental agencies comply with disclosure tax laws and agree additional actions are needed to enhance our



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

2

safeguard efforts. We appreciate your efforts in evaluating this program and your input on opportunities to further improve this process. It is our intention to establish a series of bi-monthly briefings, as well as ad hoc, if necessary, to discuss corrective actions and seek your input on proposed activities and strategies.

Attached are our detailed comments on the recommendations. If you have any comments, please call Beth Tucker, Director, Communications, Liaison and Disclosure, Small Business/Self-Employed Division at (972) 308-1676.

Attachment



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

Attachment

RECOMMENDATION 1:

The Chief Information Officer should provide management oversight for the Safeguard Review program sufficient to ensure the test plans used during Safeguard Reviews are revised and consistent with the guidance found in IRS Publication 1075.

CORRECTIVE ACTION:

We concur with this recommendation. At this time, Booz-Allen Hamilton (BAH) has revised most of the Safeguard Computer Security Evaluation Matrices, making them consistent with the requirements of NIST Special Publication 800-53. Communications to all agencies advising them that they will be held to the new standards effective October 1, 2007 are pending. The Director, Communications, Liaison and Disclosure, SB/SE Division will initiate additional changes to the guidance provided in the recently revised Publication 1075 (February 2007) to stagger reporting deadlines for Safeguard Activity Reports, as well as incorporate additional guidance for executing test plans used in Safeguard Reviews.

IMPLEMENTATION DATE:

By October 15, 2007, the Office of Safeguards will provide the revised Publication 1075 text to Forms & Publications for finalization and release.

RESPONSIBLE OFFICIAL:

Beth Tucker
Director, Communications, Liaison and Disclosure, SB/SE Division

CORRECTIVE ACTION MONITORING PLAN:

SB/SE will monitor the corrective action as part of our internal management control system.

RECOMMENDATION 2:

The Chief Information Officer should provide management oversight for the Safeguard Review program sufficient to ensure the corrective action corresponding to the follow up and monitoring of corrective actions is reopened, and a Plan of Action and Milestones (POAM) process is developed and implemented.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

2

CORRECTIVE ACTION:

We concur with this recommendation. The corrective action corresponding to the follow up and monitoring of corrective actions will be reopened, and a POAM process will be developed. The majority of development work on the newly designed automated POAM monitoring tool has been completed by the contractor.

IMPLEMENTATION DATE:

- a) By September 15, 2007, final delivery of the POAM tool will be accomplished. Once the tool is received, corrective action information from the past review cycle can be populated,
- b) By October 15, 2007, implementation of improved corrective action milestone monitoring will occur.

RESPONSIBLE OFFICIAL:

Beth Tucker
Director, Communications, Liaison and Disclosure, SB/SE Division

CORRECTIVE ACTION MONITORING PLAN:

SB/SE will monitor the corrective action as part of our internal management control system.

RECOMMENDATION 3:

The Chief Information Officer should provide management oversight for the Safeguard Review program sufficient to ensure the Safeguard Review results are provided timely to the states.

CORRECTIVE ACTION:

We concur with this recommendation. Safeguard Review results will be provided to the states within 30 calendar days of the review, but not later than 45 calendar days after the closing conference, in accordance with IRS procedures. Management will develop a monthly monitoring plan to track reports and ensure that follow-up actions have been taken on a timely basis.

IMPLEMENTATION DATE:

By August 15, 2007, the corrective procedures will be implemented..

RESPONSIBLE OFFICIAL:

Beth Tucker
Director, Communications, Liaison and Disclosure, SB/SE Division

CORRECTIVE ACTION MONITORING PLAN:

SB/SE will monitor the corrective action as part of our internal management control system.



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

3

RECOMMENDATION 4:

The Chief Information Officer should provide executive and management oversight for the Safeguard Review program sufficient to ensure task orders clearly define the staff-hours needed per task and the contractor deliverables for the remaining years of the Safeguard Review program contract.

CORRECTIVE ACTION:

We concur with this recommendation. SB/SE has assigned a task representative to work with the Contracting Officer's Technical Representative (COTR) and to manage all aspects of contract support. This task representative will ensure that work requests are written for each task area and clearly define: 1) the description of the work to be performed in accordance with the statement of work (SOW); 2) skill categories and estimated hours per category; 3) required products, due dates and specific acceptance criteria; 4) performance site; and 5) any additional government furnished equipment the contractor may need to complete the task. Work requests will be signed by the task representative, the COTR, and the contractor manager prior to starting work and upon completion of the task. At this time, we have identified six key work requests we are focusing on through December 31, 2007. In addition, we have added a Project Manager to the Safeguards staff to provide guidance, oversight, and monitoring of the program contract.

IMPLEMENTATION DATE:

July 9, 2007

RESPONSIBLE OFFICIAL:

Beth Tucker
Director, Communications, Liaison and Disclosure, SB/SE Division

CORRECTIVE ACTION MONITORING PLAN:

SB/SE will monitor the corrective action as part of our internal management control system.

RECOMMENDATION 5:

The Chief Information Officer should provide executive and management oversight for the Safeguard Review program sufficient to ensure contractor billings are monitored and contract hours allocated by task are validated to ensure funds are prudently spent.

CORRECTIVE ACTION:

We concur with this recommendation. We will ensure that contractors report hours charged to the contract by task area. As stated previously, we will ensure that a work request is in place for each task area. The assigned dedicated task



*Insufficient Attention Has Been Given to Ensure States
Protect Taxpayer Information*

4

representative will oversee our contractors and perform monthly contract reviews to ensure the accuracy of the invoices and that work authorized is completed in accordance with the work requests. During the contract review, the task representative will review the following reports, prepared by the contractor, prior to COTR review and approval: 1) Monthly Status Reports that document work performed and labor hours spent by task area; 2) work requests; and 3) invoices. Issues, if any, will be elevated to the COTR to be addressed with the contractor.

IMPLEMENTATION DATE:

July 9, 2007

RESPONSIBLE OFFICIAL:

Beth Tucker
Director, Communications, Liaison and Disclosure, SB/SE Division

CORRECTIVE ACTION MONITORING PLAN:

SB/SE will monitor the corrective action as part of our internal management control system.