



While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed

November 10, 2009

Reference Number: 2010-20-003

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

Redaction Legend:

3(a) = Identifying Information - Name of an Individual or Individuals



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 10, 2009

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED
DIVISION

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – While Effective Actions Have Been Taken to
Address Previously Reported Weaknesses in the Protection of Federal
Tax Information at State Government Agencies, Additional
Improvements Are Needed (Audit # 200920015)

This report presents the results of our followup review of a prior audit report¹ to determine whether the Internal Revenue Service (IRS) Safeguards Program has implemented sufficient policies and procedures to ensure that State Government agencies are adequately protecting Federal tax information received from the IRS. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2009 Annual Audit Plan and is part of our statutory requirements to annually review the adequacy and security of IRS information technology.

Impact on the Taxpayer

The IRS Safeguards Program is tasked with ensuring that State Government agencies receiving Federal tax information maintain adequate safeguards to protect the data from unauthorized disclosure. The IRS has taken effective actions to address two previously reported weaknesses on guidance and contract oversight in the Safeguards Program. However, improvements on the monitoring of State agencies' corrective actions and the timely reporting from reviews of State agencies are needed to ensure that Federal tax information provided to State agencies is adequately protected. These conditions increase the risk that taxpayer data are not being

¹ *Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information* (Reference Number 2007-20-134, dated August 31, 2007).



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

adequately secured and might be inappropriately accessed or used, possibly for fraudulent purposes such as identity theft.

Synopsis

In August 2007, we reported significant weaknesses in the management of the IRS Safeguards Program. Specifically, we found that 1) test plans used to conduct safeguard reviews² were not consistent with Federal guidance, 2) corrective actions stemming from safeguard reviews were not monitored in a Plan of Actions and Milestones (POA&M),³ 3) results of safeguard reviews were not provided to State Government agencies in a timely manner, and 4) contractor performance and billing were not adequately managed and verified.

In this review, we found that the IRS had corrected two of these four conditions. The IRS revised Publication 1075⁴ and the test plans to be consistent with guidelines provided in National Institute of Standards and Technology Special Publication 800-53a⁵ and implemented effective controls to manage the contract supporting the Safeguards Program. However, we believe the other two areas, the use of POA&Ms and timeliness of reporting results, were only partially corrected or not corrected at all and will continue to require management attention.

While the Safeguards Program implemented the use of POA&Ms to track security weaknesses, it did not monitor the targeted due dates of the recorded weaknesses in the POA&Ms to ensure that corrective actions were implemented in a timely manner. We identified 45 State Government agencies in the IRS POA&M tool having 1,094 security weaknesses that had not been corrected by the targeted milestone dates. These weaknesses included instances where access controls and audit trails had not been implemented effectively. The Safeguards Program conducted only a limited review of the information provided by the State agencies in their annual reports to validate that the corrective actions taken were appropriate and implemented. As such, we believe the IRS Safeguards Program is not proactively monitoring the progress of corrective actions or validating the closure of corrective actions identified during safeguard reviews of State agencies and their contractors.

² The IRS conducts safeguard reviews to evaluate State Government agencies' compliance with security procedures. These reviews generally follow test plans that contain security requirements.

³ The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

⁴ *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities*, dated October 2007, provides guidance to States regarding the policies and procedures necessary to adequately protect Federal tax information.

⁵ *Guide for Assessing the Security Controls in Federal Information Systems*, dated July 2008, provides guidelines for building security assessment plans and comprehensive procedures for assessing the effectiveness of security controls employed in information systems in the Federal Government.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

In addition, we determined that safeguard review reports continue to be issued in an untimely manner. For safeguard reviews conducted in Fiscal Year 2008, the Safeguards Program issued 66 of 78 draft reports in an average of 106 calendar days after the closing conferences. As of June 30, 2009, the remaining 12 draft reports for Fiscal Year 2008 had not yet been issued to the recipient agencies and their contractors. These reports averaged 354 calendar days past the closing conference dates.

Recommendations

We recommended that the Director, Safeguards, Small Business/Self-Employed Division, 1) revise existing policies, as necessary, to require State agencies and their contractors to provide sufficient documentation on a more frequent basis to support that corrective actions were taken to address reported computer security weaknesses, 2) complete planned personnel actions so that adequate staffing is available to proactively monitor and validate the corrective security actions taken by State agencies and their contractors, and 3) continue to use the recently implemented monitoring tool and complete the training of new staff to increase the efficiency of the reporting process.

Response

IRS management agreed with our recommendations. Publication 1075 will be revised to require the State Government agencies to report the status of their actions to address outstanding findings on a semiannual basis and provide documentary verification when closing high-priority findings. In addition, a recruitment action to staff a full-time position dedicated to the monitoring of corrective actions taken by State agencies and their contractors will be completed. Lastly, the Office of Safeguards will continue to utilize the inventory monitoring tool and complete the training of new staff.

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) 622-8510.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Table of Contents

Background	Page 1
Results of Review	Page 3
The Safeguards Program Has Corrected Prior Weaknesses on Its Test Plans and Contract Oversight.....	Page 3
The Safeguards Program Was Not Adequately Monitoring and Verifying Whether State Government Agencies Are Implementing Corrective Actions on Identified Computer Security Weaknesses.....	Page 4
<u>Recommendation 1</u> :.....	Page 5
<u>Recommendation 2</u> :.....	Page 6
The Results of Safeguard Reviews of State Government Agencies Continue to Be Reported in an Untimely Manner	Page 6
<u>Recommendation 3</u> :.....	Page 7
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 8
Appendix II – Major Contributors to This Report	Page 10
Appendix III – Report Distribution List	Page 11
Appendix IV – Management’s Response to the Draft Report	Page 12



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Abbreviations

IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Actions and Milestones



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Background

The Internal Revenue Code¹ authorizes the Internal Revenue Service (IRS) to disclose Federal tax information to various State Government agencies for the purpose of tax administration. For example, State tax agencies can use Federal tax information to identify individuals who have not filed State tax returns, determine whether discrepancies exist in the reporting of income, locate delinquent taxpayers, and determine whether IRS adjustments have State tax implications.

Due to Federal Government requirements to protect tax information and the concerns over the potential misuse of unprotected data for identity theft, State Government agencies are required to have adequate controls in place to prevent unauthorized disclosures. *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities* (IRS Publication 1075, dated October 2007) provides guidance to State agencies regarding the policies and procedures necessary to adequately protect Federal tax information. Before a State agency receives Federal tax information, it must submit a formal report that describes how it will protect and safeguard the tax information. In addition, State agencies that receive Federal tax information are required to file an annual report to describe any changes to their safeguard procedures, advise the IRS of future actions that will affect safeguard procedures, and certify that they are protecting the data.

The Safeguards Program within the Communications, Liaison, and Disclosure organization of the IRS Small Business/Self-Employed Division is responsible for managing and providing oversight to State Government agencies receiving Federal tax information. To ensure the information is adequately protected, the Safeguards Program is responsible for conducting safeguard reviews² at least once every 3 years of each State agency receiving Federal tax information and is responsible for evaluating the State agencies' compliance with security procedures. During its onsite reviews, the Safeguards Program uses test plans that address the security requirements for State agencies processing and storing Federal tax information on different computing platforms, including Windows, UNIX, and IBM mainframe computers.

In February 2003, we issued a report³ which concluded that Federal tax information was at risk while in the possession of State Government tax agencies. In September 2005, we issued a followup report⁴ that raised specific concerns regarding the physical security, user account

¹ Internal Revenue Code Section 6103 (2008).

² The IRS conducts safeguard reviews to evaluate State Government agencies' compliance with security procedures. These reviews generally follow test plans that contain security requirements.

³ *Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk* (Reference Number 2003-20-064, dated February 21, 2003).

⁴ *Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 30, 2005).



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

management, access controls, audit trails, intrusion detection, and firewall systems at all four State agencies we visited. These weaknesses placed Federal tax information at increased risk of unauthorized use or theft.

In August 2007, we conducted another followup review⁵ and reported significant weaknesses in the management of the IRS Safeguards Program. Specifically, we reported that 1) test plans used to conduct safeguard reviews were not consistent with Federal guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53a,⁶ 2) corrective actions stemming from safeguard reviews were not monitored, 3) results of safeguard reviews were not provided to State Government agencies in a timely manner, and 4) contractor performance and billing were not adequately managed and verified.

This review was performed at the Small Business/Self-Employed Division Safeguards Program office in the IRS Headquarters in Washington, D.C., during the period March through August 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

⁵ *Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information* (Reference Number 2007-20-134, dated August 31, 2007).

⁶ *Guide for Assessing the Security Controls in Federal Information Systems*, dated July 2008, provides guidelines for building security assessment plans and comprehensive procedures for assessing the effectiveness of security controls employed in information systems in the Federal Government.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Results of Review

During our August 2007 review, we reported significant weaknesses in the management of the IRS Safeguards Program. Specifically, we identified four key areas needing management attention.

1. To be consistent with Federal Government computer security guidance found in NIST Special Publication 800-53a, management needed to revise its test plans used during its onsite reviews of State agencies.
2. To increase its management oversight of the contract supporting the Safeguards Program, management needed to clearly define task orders,⁷ staff hours, and contractor deliverables, as well as closely monitor contractor billings.
3. To monitor and validate State Governments' corrective actions of reported computer security weaknesses, management needed to develop and implement a Plan of Actions and Milestones (POA&M)⁸ process.
4. To comply with the 45-day reporting time period, management needed to improve its timeliness of reporting the results of its reviews to State Government agencies.

In July 2007, the Safeguards Program was moved from the Modernization and Information Technology Services Cybersecurity organization to the Small Business/Self-Employed Division. The new management staff took immediate actions to address these weaknesses. In our current review, we noted improvements in the first two areas. IRS Publication 1075 and the test plans have been revised to be consistent with Federal guidelines, and effective controls have been implemented to manage the contract supporting the Safeguards Program. However, we believe the other two areas, the use of POA&Ms and the timeliness of reporting results, were only partially corrected or not corrected at all and will continue to require management attention.

The Safeguards Program Has Corrected Prior Weaknesses on Its Test Plans and Contract Oversight

During our 2007 review, we determined that test plans the Safeguards Program management approved for use during its computer security onsite reviews of State Government agencies had not been updated to include many of the control areas described in NIST Special

⁷ A task order is an order for services placed against an established contract.

⁸ The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.



***While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed***

Publication 800-53a. Until these documents were revised, the IRS could not be assured that State agencies were adequately protecting Federal tax information. We also identified significant weaknesses in the management of the contract supporting the Safeguards Program, including task orders that were signed after the work had been performed, task orders that did not contain estimates of the hours that were required to perform the tasks, no process in place to validate the hours billed on contractor invoices, and payment vouchers that were not adequately reviewed and approved prior to payment. Due to the poor contract oversight provided by the IRS, (b) (3)(a) and subsequently referred our concerns (b) (3)(a) to the Treasury Inspector General for Tax Administration Office of Investigations for further review. (b) (3)(a)

In our current review, we reviewed all 13 test plans used during safeguard reviews. We compared the test plans and the IRS Publication 1075 to NIST Special Publication 800-53a and determined that these documents contained the necessary controls provided in the guidance documents. We also reviewed the contract's Statement of Work, related task orders, and invoices for Fiscal Years 2008 and 2009. We determined that the task orders clearly defined the work to be performed and included key information, such as skill categories and estimated hours per category, deliverables, due dates for deliverables, specific acceptance criteria, and sites where work would be performed. The task orders and invoices were appropriately reviewed and approved by the IRS prior to payment of the invoices. The IRS had also implemented scheduled weekly and monthly conference calls with the contractor to discuss performance and billing status.

***The Safeguards Program Was Not Adequately Monitoring and
Verifying Whether State Government Agencies Are Implementing
Corrective Actions on Identified Computer Security Weaknesses***

IRS procedures require that POA&Ms be used to track the status of resolution of all computer security weaknesses and that the correction of each weakness be verified before closing that item on the POA&M. Further, the Safeguards Program POA&M methodology document states that, for each State Government agency, POA&M data should be continually monitored as significant events occur and completed milestones should be updated on the POA&M report according to specified time periods. Because some of the POA&M resolution time periods are less than 1 year, State agencies are encouraged to send POA&M updates regarding closures to the safeguard review team when they make their own updates.

In our 2007 review, we determined that the Safeguards Program had not implemented a POA&M process to monitor security weaknesses identified during safeguard reviews. In our current review, we found that the Safeguards Program conducts safeguard reviews of the various State agencies that receive Federal tax information, records reported weaknesses in the Safeguards



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Program POA&M management tool, and receives annual updates from the agencies explaining what corrective actions they have taken.

However, the Safeguards Program does not monitor the targeted due dates of the recorded weaknesses to ensure that corrective actions are implemented in a timely manner. We identified 45 State agencies in the IRS POA&M tool having 1,094 security weaknesses that had not been corrected by the targeted milestone dates. These weaknesses included instances where access controls and audit trails had not been implemented effectively. The Safeguards Program conducts only a limited review of the information provided by the State agencies in their annual reports to validate that corrective actions taken were appropriate and implemented. Therefore, we believe the Safeguards Program is not proactively monitoring the progress of corrective actions or validating the closure of corrective actions identified during safeguard reviews of State agencies and their contractors.

For its monitoring efforts, the Safeguards Program places the burden for monitoring corrective actions on the State agencies and their contractors that receive Federal tax information. As for validating closure of corrective actions, the Safeguards Program POA&M methodology does not include the validation of corrective actions prior to their closure on the POA&M. When we presented our concerns over this issue, Safeguards Program management informed us that they had planned to revise IRS Publication 1075 to increase the frequency of POA&M reporting by State agencies. However, the specifics of the time periods or format for the new reporting requirements have not been defined. Safeguards Program management also explained that they do not currently have the staff needed to proactively monitor the POA&Ms. Management plans to fill a staff position that would be dedicated to proactively managing the corrective actions in the POA&M tool.

Given limited oversight by the Safeguards Program, State Government agencies and their contractors might not take appropriate corrective actions within a reasonable time period to correct security weaknesses identified in safeguard reviews. Inaction or inappropriate actions by State agencies and their contractors increase the risk that Federal tax information might not be adequately protected and might be inappropriately accessed or used, possibly for fraudulent purposes such as identity theft.

Recommendations

The Director, Safeguards, should:

Recommendation 1: Revise existing policies, as necessary, to require State agencies and their contractors to provide sufficient documentation on a more frequent basis to support that corrective security actions were taken to address reported computer security weaknesses.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Management's Response: IRS management agreed with this recommendation. Revisions to IRS Publication 1075 will require agencies to 1) report the status of their actions to address outstanding findings on a semiannual basis and 2) provide documentary verification when closing high-priority findings.

Recommendation 2: Complete planned personnel actions so that adequate staffing is available to proactively monitor and validate the corrective security actions taken by State agencies and their contractors.

Management's Response: IRS management agreed with this recommendation. A recruitment action has been initiated to staff a full-time position dedicated to the monitoring of corrective actions taken by the State agencies and their contractors.

The Results of Safeguard Reviews of State Government Agencies Continue to Be Reported in an Untimely Manner

IRS procedures state that safeguard review reports should be provided to the State agency and/or to its contractors promptly after the conclusion of the onsite portion of the review to convey the IRS' commitment to ensuring the confidentiality of the Federal tax information and return information. The interim safeguard review reports should be issued within 45 calendar days after the closing conference.

During our 2007 review, we reported that the Safeguards Program issued safeguard reports during Fiscal Years 2006 and 2007 in an average of 81 calendar days after completion of onsite reviews. We attributed the late issuance of reports to a lack of management attention to the process.

In this review, we determined that the IRS has increased its management attention to the reporting process. Safeguards Program management provided us with the spreadsheet tool they use to monitor the status of reports. In the prior audit, management did not use similar monitoring tools.

While management attention has increased, reports still continue to be issued in an untimely manner. For safeguard reviews conducted in Fiscal Year 2008, the Safeguards Program issued 66 of 78 draft reports in an average of 106 calendar days after the closing conferences. As of June 30, 2009, the remaining 12 draft reports for Fiscal Year 2008 had not been issued to the recipient agencies and their contractors and averaged 354 calendar days after the closing conference dates. With these delays, security weaknesses identified in safeguard reviews might not be addressed for months after the reviews, increasing the risk that Federal tax information might not be adequately protected and, therefore, could be inappropriately accessed or used.

We believe the most significant cause for the delays in reporting was a turnover in staff in the Safeguards Program. At the end of Fiscal Year 2008, two experienced staff employees retired



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

and three new employees were hired. The new hires have devoted considerable time to completing the training program established by the Safeguards Program. Safeguards Program management believes that once the new hires are trained, and they are available to devote their full attention to the review process, the timeliness issue will improve.

Recommendation

The Director, Safeguards, should:

Recommendation 3: Continue to use the recently implemented monitoring tool and complete the training of new staff to increase the efficiency of the reporting process.

Management's Response: IRS management agreed with this recommendation. They will continue to utilize the inventory monitoring tool, focus on improving the timely issuance of reports, and complete the training of new employees.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to follow up on a prior audit report¹ and determine whether the IRS Safeguards Program has implemented sufficient policies and procedures to ensure that State Government agencies are adequately protecting Federal tax information received from the IRS. To accomplish our objective, we:

- I. Determined whether test plans used to conduct safeguard reviews are consistent with applicable guidance, including IRS Publication 1075² and NIST Special Publication 800-53a.³
 - A. Reviewed all 13 test plans being used during safeguard reviews.⁴
 - B. Compared test plans with IRS Publication 1075 and NIST Special Publication 800-53a.
 - C. Discussed any discrepancies noted in Step I.B. with Safeguards Program management to determine reasons for variances in the documents.
- II. Determined whether a sound oversight program has been implemented to conduct safeguard reviews, identify weaknesses and corrective actions, and monitor corrective actions to completion.
 - A. Reviewed milestone information for safeguard reviews to determine whether:
 1. Reviews are started as scheduled.
 2. Reviews are completed in a timely manner.
 3. Results are provided to State agencies in a timely manner.

¹ *Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information* (Reference Number 2007-20-134, dated August 31, 2007).

² *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities*, dated October 2007, provides guidance to States regarding the policies and procedures necessary to adequately protect Federal tax information.

³ *Guide for Assessing the Security Controls in Federal Information Systems*, dated July 2008, provides guidelines for building security assessment plans and comprehensive procedures for assessing the effectiveness of security controls employed in information systems in the Federal Government.

⁴ The IRS conducts safeguard reviews to evaluate State Government agencies' compliance with security procedures. These reviews generally follow test plans that contain security requirements.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

- B. Determined whether the Safeguard Program is:
 - 1. Tracking weaknesses and corrective actions resulting from safeguard reviews using a POA&M⁵ process.
 - 2. Closely monitoring the POA&Ms to ensure that corrective actions are implemented.
 - 3. Properly validating corrective actions prior to closing them out on the POA&Ms.
 - C. Discussed any issues identified from audit Steps II.A. and II.B. with Safeguards Program management to determine why issues exist.
 - D. Assessed the effect of any weaknesses identified during completion of audit Steps II.A. and II.B.
- III. Determined whether contractor support for the Safeguards Program is adequately managed.
- A. Determined whether work requests are written for each task and clearly define the work to be performed as outlined in the Statement of Work (including skill categories and estimated hours per category; required products, due dates, and specific acceptance criteria; performance sites; and any Government-furnished equipment needed by the contractor).
 - B. Determine whether work requests are reviewed and approved by IRS management.
 - C. Discussed the contractor oversight process with Safeguards Program management, reviewed evidence that contractor performance is being reviewed on a regular basis, and determined whether the review process appears effective.
 - D. Reviewed contractor invoices and documentation to determine whether they are adequately reviewed prior to approval by IRS management.
 - E. Discussed any issues identified from audit Steps III.A. through III.D. with Safeguards Program management to determine why the issues exist.
 - F. Assessed the effect of weaknesses identified during completion of audit Steps III.A. through III.D.

⁵ The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Acting Director
Carol Taylor, Audit Manager
Myron Gulley, Senior Auditor
Louis Lee, Senior Auditor
Monique Queen, Information Technology Specialist



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner, Small Business/Self-Employed Division SE:S
Director, Communications, Liaison, and Disclosure, Small Business/Self-Employed Division
SE:S:CLD
Director, Safeguards, Small Business/Self-Employed Division SE:S:CLD:S
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Commissioner, Small Business/Self-Employed Division SE:S



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Appendix IV

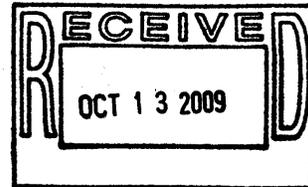
Management's Response to the Draft Report



COMMISSIONER
SMALL BUSINESS/SELF-EMPLOYED DIVISION

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

October 8, 2009



MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Christopher Wagner
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – While Effective Actions Have Been Taken to
Address Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed (Audit No. 200920015)

Thank you for the opportunity to review the draft report titled "While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed." We agree with the recommendations outlined in the report regarding the further improvements needed and are already taking steps to address them. We appreciate your recognition of the significant actions already taken to effectively address previously reported weaknesses.

Attached is a detailed response outlining our corrective actions. If you have questions, please call me at (202) 622-0600 or Janet Miner, Director, Office of Safeguards, Small Business/Self Employed Division, at (202) 622-6807.

Attachment



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

Attachment

RECOMMENDATION 1:

The Commissioner, Small Business/Self-Employed Division, should revise existing policies, as necessary, to require State agencies and their contractors to provide sufficient documentation on a more frequent basis to support that corrective security actions were taken to address reported computer security weaknesses.

CORRECTIVE ACTIONS:

We agree with this recommendation. Our approach for resolving this recommendation is based upon discussions with TIGTA personnel on the most effective manner to monitor outstanding corrective actions more effectively without placing undue administrative burden on state governmental agencies which are already facing significant resource constraints. Revisions to the current version of Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, which are scheduled for a February 2010 release, will require agencies to: 1) report the status of their actions to address outstanding findings on a semi-annual basis; and 2) provide documentary verification when closing high priority findings.

IMPLEMENTATION DATE:

February 15, 2010

RESPONSIBLE OFFICIAL:

Director, Office of Safeguards (SB/SE Division).

CORRECTIVE ACTION(S) MONITORING PLAN:

The Director, Office of Safeguards will monitor the status and advise the Director, Communication, Liaison and Disclosure of any delays in implementing.

RECOMMENDATION 2:

The Commissioner, Small Business/Self-Employed Division, should complete planned personnel actions so that adequate staffing is available to proactively monitor and validate corrective security actions taken by State agencies and their contractors.

CORRECTIVE ACTIONS:

We agree with this recommendation. The Director, Office of Safeguards has already initiated a recruitment action to staff a full-time position dedicated to the monitoring of corrective actions taken by the state agencies and their contractors.

IMPLEMENTATION DATE:

January 15, 2010

RESPONSIBLE OFFICIAL:

Director, Office of Safeguards (SB/SE Division).



*While Effective Actions Have Been Taken to Address
Previously Reported Weaknesses in the Protection of
Federal Tax Information at State Government Agencies,
Additional Improvements Are Needed*

2

CORRECTIVE ACTION(S) MONITORING PLAN:

The Director, Office of Safeguards will monitor the status and advise the Director, Communication, Liaison and Disclosure of any delays in implementing.

RECOMMENDATION 3:

The Commissioner, Small Business/Self-Employed Division, should continue the use of the recently implemented monitoring tool and complete the training of the new staff to increase the efficiency of the reporting process.

CORRECTIVE ACTIONS:

We agree with this recommendation. The Director, Office of Safeguards will continue to utilize the inventory monitoring tool, focus on improving the timely issuance of reports and complete the training of the new staff.

IMPLEMENTATION DATE:

January 15, 2010

RESPONSIBLE OFFICIAL:

Director, Office of Safeguards (SB/SE Division).

CORRECTIVE ACTION(S) MONITORING PLAN:

The Director, Office of Safeguards will monitor the status and advise the Director, Communication, Liaison and Disclosure of any delays in implementing.