Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected

September 2005

Reference Number: 2005-20-184

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 30, 2005

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Audit # 200520005)

This report presents the results of our review of security of Federal tax information provided to State agencies. The overall objective of this review was to determine whether State tax agencies were protecting Federal tax information from unauthorized use and disclosure.

Section 6103 of the Internal Revenue Code[1] requires the Internal Revenue Service (IRS) to disclose Federal tax information to various State and Federal Government agencies. State tax agencies can use this 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. Due to the sensitivity of Federal tax information and the potential for its misuse for identity theft, the States are required to have adequate controls in place to prevent unauthorized disclosures of the tax information.

Synopsis

In February 2003, we issued a report[2] in which we concluded that Federal tax information was at risk while in the possession of State tax agencies. We recommended the IRS broaden the scope of its reviews of States receiving Federal tax information to include a more comprehensive review of computer security and hire or develop an adequate number of technically proficient staff to conduct those reviews. The IRS agreed with each of our recommendations.

[1] Internal Revenue Code § 6103 (2003).
[2] *Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk* (Reference Number 2003-20-064, dated February 2003).

In this review, we visited four large State tax agencies to which the IRS sends Federal tax information. At all four agencies, we identified significant weaknesses in physical security, user account management, access controls, audit trails, intrusion detection, and firewall systems. These weaknesses place Federal tax information at increased risk of unauthorized use or theft. Hackers and unscrupulous State government employees could exploit these security weaknesses to gain unauthorized access to tax data.

The IRS requires the States to review security controls and submit the test results annually to the IRS. The reviews conducted by the States, however, do not adequately assess whether security controls are in place. The reviews performed by the four State tax agencies we visited did not identify the security weaknesses we found. In addition, the scopes of the States' reviews did not comply with the Federal Information Security Management Act (FISMA),[3] which requires users of Federal tax data to test security controls annually using National Institute of Standards and Technology (NIST)[4] guidance.

The IRS has made improvements in its reviews of the States' security controls. The most significant change was reassigning responsibility for these reviews from the Office of Governmental Liaison and Disclosure, within the Communications and Liaison Division, to the Office of Mission Assurance and Security Services (MA&SS).

MA&SS organization computer security specialists followed guidelines, prepared by a contractor, in reviewing the security controls at the States. These guidelines represent a significant improvement from past practices by testing for more vulnerabilities. However, they still do not comply with the NIST guidelines used for testing information systems in accordance with the FISMA.

Additionally, the management information system used by the MA&SS organization to monitor the status of corrective actions does not have the capability to record the corrective actions or the proposed completion dates of those actions. The States, then, are not held accountable for addressing weaknesses found during their tests and the tests conducted by the MA&SS organization.

Recommendations

To reduce the opportunities for unauthorized use of Federal tax information at State agencies, we recommended the Chief, MA&SS, obtain a formal decision from the Office of Management and Budget (OMB) as to the application of the FISMA computer security requirements to State agencies that receive Federal tax information. We recommended the Chief, MA&SS, require

[3] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[4] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

States to submit more useful and indepth annual self-assessments using *Recommended Security Controls for Federal Information Systems* (NIST Special Publication 800-53). These self-assessments should be used by the MA&SS organization to better focus the scope of its reviews, resulting in a more efficient use of resources. Additionally, if FISMA requirements are determined to apply to State agencies receiving Federal tax information, the Chief, MA&SS, should require the States to submit the same documents required by Federal Government agencies to enable the MA&SS organization to monitor corrective actions and follow up on prior issues identified.

To improve the scope of reviews over States' security controls, we recommended the Chief, MA&SS, ensure the IRS' reviews of States follow NIST Special Publication 800-53 guidance. Finally, we recommended the Chief, MA&SS, assign additional staffing to oversee the States' controls.

Response

The Chief, MA&SS, does not believe that FISMA requirements apply to State agencies receiving Federal tax information primarily because the agencies do not use the tax information on behalf of the IRS. Therefore, the Chief, MA&SS, disagreed with our first recommendation and did not seek a formal opinion from the OMB on this matter. Although the Chief, MA&SS, disagreed that FISMA requirements apply to the States, he agreed to revise *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075) to incorporate the recommended security controls described in NIST Special Publication 800-53. Also the MA&SS organization will use Plans of Actions and Milestones as part of a new process to better manage recommended corrective actions. In addition, the Chief, MA&SS, will improve the scope of IRS Safeguard Reviews by incorporating appropriate NIST Special Publication 800-53 security controls into the computer security Safeguard Review process. Finally, the Chief, MA&SS, agreed with our recommendation to assign additional staffing to oversee the States' controls and will determine the staffing needs for the additional workload items presented in this report. In the interim, MA&SS organization personnel have been identified to assist in conducting the computer security reviews. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment

We do not agree with the IRS that FISMA requirements do not apply to State agencies receiving Federal tax information. Based on FISMA reporting guidance provided by the OMB for Fiscal Year 2005, we believe the OMB intends for the FISMA requirements to apply to State agencies receiving Federal tax information. To resolve this matter, we have requested a formal opinion from the OMB.

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

Table of Contents

Background

Section 6103 of the Internal Revenue Code[1] requires the Internal Revenue Service (IRS) to disclose Federal tax information to various State and Federal Government agencies. State tax agencies can use this 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.

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 Report describes how the State will protect and safeguard the tax information. In addition, States are required to annually file a Safeguard Activity Report to report 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 Federal Information Security Management Act (FISMA)[2] also requires the IRS to provide oversight to ensure the States have adequate security controls in place to protect Federal tax information. The IRS is responsible for overseeing security over Federal tax information for 276 Federal Government and State entities. Balancing priorities is clearly an issue; however, the Office of Management and Budget (OMB) has stressed the need for oversight of entities receiving sensitive Federal Government information and evaluates agencies' oversight activities through the FISMA reporting process.

Prior to October 2003, the IRS Office of Governmental Liaison and Disclosure, within the Communications and Liaison Division, had primary responsibility for ensuring security over tax information provided to State and Federal Government agencies. In October 2003, this oversight responsibility was shifted to the Office of Mission Assurance and Security Services (MA&SS).

In February 2003, we issued a report[3] in which we concluded that Federal tax information was at risk while in the possession of State agencies. We recommended the IRS broaden the scope of its reviews of States receiving Federal tax information to include a more comprehensive review of computer security and hire or develop an adequate number of technically proficient staff to conduct those reviews. The IRS agreed with each of our recommendations.

---

[1] Internal Revenue Code § 6103 (2003).
[2] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[3] *Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk* (Reference Number 2003-20-064, dated February 2003).

This review was performed at the MA&SS organization offices in the IRS National Headquarters in Washington, D.C., during the period December 2004 through May 2005. We also visited and reviewed security at four large State tax agencies in Michigan, Illinois, New York, and Texas that receive Federal tax information. We did not review the security of the data being shared with nontax State agencies or Federal Government agencies. 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.

Results of Review

Computer Weaknesses Continue to Exist at State Tax Agencies, Jeopardizing the Security of Federal Tax Information

We identified significant security weaknesses at all four State tax agencies we reviewed. These weaknesses provide opportunities for hackers, disgruntled employees, and contractors to access Federal tax information for unauthorized use and identity theft purposes. The weaknesses continue because the States' self-assessments of security controls have not been adequate. In addition, while the IRS has improved its reviews of States' security controls, more oversight is needed.

Controls to prevent hackers from attacking States' networks from the Internet are not adequate

Security weaknesses at Internet connections give hackers opportunities to exploit and gain unauthorized entry into the internal network. In accordance with the FISMA, the National Institute of Standards and Technology (NIST)[4] requires Federal Government agencies and those entities receiving Federal tax information to protect networks at Internet connections. Generally, firewall computers and routers stop traffic from traveling from the Internet to an internal, trusted network. Intrusion detection systems detect inappropriate, incorrect, or unusual activity on a network.

We identified security weaknesses at Internet connections at all four State tax agencies we reviewed. The following weaknesses result in the States being unnecessarily vulnerable to attacks by hackers:

- Firewall computers were not optimally configured and maintained to minimize the possibility of an attack.
- Password controls on firewalls and routers were weak. User names and passwords were not required on some equipment and were sometimes shared by system administrators. Unique user names and passwords help identify persons responsible for changes to router settings. These weaknesses could allow unauthorized personnel to access connection components and make unauthorized configuration changes.

[4] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

- Activity logs and audit trail logs that contain details of accesses to systems were not reviewed and analyzed. Consequently, the States were hindered in identifying and investigating potential attacks.
- Intrusion detection capabilities had not been installed at all connections. Intrusion detection systems provide an organization the ability to monitor activity on its network and look for suspicious and unauthorized actions.

Controls to prevent disgruntled employees and contractors from exploiting States' networks are not adequate

Employees and contractors usually have more knowledge of systems than hackers and, as a result, can often cause more damage. Sufficient management, operational, and technical controls are required for each system to limit the opportunities for misuse of data. We identified security weaknesses at all four State tax agencies that increased the risk that disgruntled employees and contractors with access to the States' networks could gain unauthorized access to Federal tax information. Specifically:

- Compact discs containing Federal tax information were stored in cabinets that remained unlocked during work hours. Packages containing tapes with tax information were opened in the mail room and left unsecured prior to delivery. Inventory controls were not in place for a significant number of compact discs on hand and backup tapes stored offsite. Employees' duties were not separated among receiving, accounting for, and inventorying tapes. These practices make the tax information more susceptible to theft.
- States could not determine when employees last accessed systems containing Federal tax information.
- Employees who no longer needed access to systems still had active user accounts.
- End users' requests for access to Federal tax information were not documented.
- One State had not provided logon warning messages to end users regarding the consequences of misusing or inappropriately accessing Federal tax information.
- None of the four State tax agencies reviewed audit trails to detect inappropriate access to Federal tax information.

The States' self-assessments of security controls have not been adequate

We believe State agencies, as users of Federal tax information, are obligated to comply with the FISMA self-assessment security control requirements. We suggest States use *Recommended*

Security Controls for Federal Information Systems (NIST Special Publication 800-53) when performing self-assessments of security controls. This Publication is applicable to all computers and systems containing sensitive data. It clearly outlines key security issues and guides users to determine whether policies and procedures have been developed, implemented, and tested. States should be required to submit these self-assessments annually with their Safeguard Activity Reports. The MA&SS organization could then use the self-assessments to focus the scope of its reviews and potentially reduce the staffing required to test computer security controls.

The most recent Safeguard Activity Reports prepared by the four State tax agencies we reviewed do not adequately assess whether security controls are in place. None of the four agencies used the NIST guidance, and the self-assessments they performed did not identify the security weaknesses we found. The self-assessments were limited in scope and did not adequately describe the steps taken to evaluate the controls.

These cursory reviews do not provide assurance to the IRS that States are meeting their responsibilities for providing adequate computer security controls to protect Federal tax information. The IRS has accepted the annual reports without enforcing existing requirements for reporting on controls.

The IRS Safeguard Reviews are inadequate and incomplete

The IRS' most recent Safeguard Reviews of the four State tax agencies did not identify the weaknesses we found. The IRS did not provide sufficient staffing to review States' security controls, and the reviews that were conducted were not sufficiently indepth to identify all critical control weaknesses. In addition, the IRS did not use methods required by the FISMA to monitor actions to correct identified weaknesses.

One of the major considerations behind the transfer of responsibility for overseeing States' security controls to the MA&SS organization was the availability of technically proficient information technology staff to conduct the technical portions of the IRS Safeguard Reviews. However, due to budget constraints, only two computer security specialists were assigned to the MA&SS organization's Safeguards Program. Both specialists had been reassigned from the Office of Governmental Liaison and Disclosure. The only additional staff provided by the MA&SS organization has been two individuals to perform ad hoc physical security reviews. To supplement its staff, the MA&SS organization acquired contractor support for the technical portions of the Safeguard Reviews. However, IRS procedures require the MA&SS organization to review the security over Federal tax information at least once every 3 years for approximately 276 Federal Government and State entities, thus requiring approximately 90 reviews each year. In Fiscal Year 2004, the IRS conducted only 66 reviews, which included 26 State tax agencies, 32 State child support and welfare agencies, and 8 Federal Government entities. Additional staffing is needed to meet the IRS' oversight responsibilities.

In addition, the scope of the reviews was not sufficient. The contractor hired by the IRS developed 15 matrices that are used by the MA&SS organization specialists and the contractor staff when evaluating the States' computer security controls. The matrices are designed to evaluate operating systems most commonly found in the States such as Windows 2000, Windows NT, and UNIX.

The matrices are an improvement from past practices because they test for more vulnerabilities. However, the matrices do not address controls prescribed in NIST Special Publication 800-53. Application controls are the last line of defense in protecting the IRS' sensitive data. In addition, several controls that require human involvement are still not addressed, such as ensuring employees with significant security responsibilities are adequately trained. The matrices also do not address privacy issues, such as the unauthorized browsing and/or theft of Federal tax information while in the custody of the States.

We also determined the MA&SS organization's management information system does not track the corrective actions planned by the agencies under review, nor does it track the actual corrective action completion dates. The FISMA requires agencies to formulate Plans of Actions and Milestones to record all identified security weaknesses, list specific corrective actions to address those weaknesses, and include dates by which those corrective actions will be completed.

The management information system used by the MA&SS organization to monitor the status of corrective actions does not have the capability to record the corrective actions or the proposed completion dates of those actions. The States, then, are not held accountable for addressing weaknesses found during their tests and the tests conducted by the MA&SS organization. As a result, the IRS cannot be certain that deficiencies found during Safeguard Reviews are timely and efficiently corrected.

Recommendations

To reduce the opportunities for unauthorized use of Federal tax information at State agencies, the Chief, MA&SS, should:

Recommendation 1: Obtain a formal decision from the OMB as to the application of the FISMA computer security requirements for systems at State agencies that receive Federal tax information.

> ***Management's Response:*** The Chief, MA&SS, disagreed with this recommendation stating that, currently, FISMA legislation and the applicable NIST standards are not mandated for the State agencies receiving Federal tax information because the State agencies do not use the information for the benefit, aid, or support of the IRS. In addition, State agencies are not accessing, connecting to, or using IRS major information

systems to collect, maintain, process, store or transmit this information for, or on behalf of, the IRS.

Office of Audit Comment: We do not agree with the IRS that FISMA requirements do not apply to State agencies receiving Federal tax information. FISMA reporting guidance provided by the OMB states, "… agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc." Later in the same paragraph, the guidance states, "Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems." Although the States may not be using the data on behalf of the IRS, they clearly have privileged access to the data and, therefore, we believe the OMB intends for the States to be included in the IRS' security program. To resolve this issue, we have requested a formal opinion from the OMB.

Recommendation 2: If States receiving Federal tax information are required to comply with the FISMA requirements, require States to submit more useful and indepth self-assessments annually, using NIST Special Publication 800-53, with their Safeguard Activity Reports. These self-assessments should be used by the MA&SS organization to better focus the scope of its Safeguard Reviews, resulting in a more efficient use of resources. Additionally, as part of the oversight of entities receiving Federal tax information, the Chief, MA&SS, should require the States to submit Plans of Actions and Milestones to track corrective actions at the States and follow up on prior issues identified.

Management's Response: Although the Chief, MA&SS, disagreed that the FISMA requirements apply to State agencies receiving Federal tax information, he agreed to revise *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075) to incorporate the recommended security controls described in the NIST Special Publication 800-53. The MA&SS organization will use Plans of Actions and Milestones as part of a new process to better manage recommended corrective actions.

Recommendation 3: Improve the scope of the IRS Safeguard Reviews by following NIST Special Publication 800-53 guidance.

Management's Response: The Chief, MA&SS, agreed with this recommendation and will incorporate NIST Special Publication 800-53 standards into the computer security Safeguard Review process. However, the Chief, MA&SS, stated that, because the States are not subject to the FISMA, it may not be practical to incorporate all of the recommended controls from NIST Special Publication 800-53 into the Safeguard Review methodology. IRS Publication 1075 will be updated to incorporate the viable

recommended security controls in NIST Special Publication 800-53, allowing for some flexibility in the requirements imposed for the States as appropriate.

Recommendation 4: Assign more staffing to the MA&SS organization's Safeguards Program so adequate oversight can be provided to the States.

Management's Response: The Chief, MA&SS, agreed with this recommendation and will determine the staffing needs for the additional workload items presented in this report. In the interim, MA&SS organization personnel have been identified to assist in conducting the computer security reviews.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to determine whether State tax agencies were protecting Federal tax information from unauthorized use and disclosure. To accomplish this objective, we:

I. Visited four large State tax agencies located in Michigan, Illinois, New York, and Texas to review physical and computer security controls over Federal tax information. From a population of 50 States, we selected the 4 most populous States that the IRS had not scheduled for review in Fiscal Years 2004 and 2005.

   A. Reviewed the States' physical security over Federal tax information.

   B. Reviewed the States' controls over access to Federal tax information.

   C. Determined whether the States used audit trails to detect improper accesses to computers used to process and store Federal tax information. We determined whether audit trails were turned on and reviewed on a regular basis.

   D. Determined whether the States used firewalls to prevent improper access to computers that process and store Federal tax information.

   E. Determined whether intrusion detection systems were used to continuously monitor systems that process and store Federal tax information and how intrusion detection systems were deployed.

   F. Determined the extent to which the States self-reviewed their systems.

II. Reviewed coverage given to computer security during the Internal Revenue Service Safeguard Reviews.

   A. Reviewed procedures and guidelines used by Internal Revenue Service reviewers and computer security specialists for performing Safeguard Reviews and for performing the computer security portion of Safeguard Reviews.

   B. Reviewed the coverage given to computer security during Safeguard Reviews. We obtained documentation on Safeguard Reviews for the four State tax agencies.

III. Reviewed the Mission Assurance and Security Service organization's monitoring of corrective actions. We determined how it ensured State tax agencies implemented meaningful and timely corrective actions to computer security deficiencies in Safeguard Review Reports.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Gerald H. Horn, Audit Manager
Dan Ardeleano, Senior Auditor
Bret D. Hunter, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Joan Raniolo, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn.: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaison: Chief, Mission Assurance and Security Services OS:MA

Appendix IV

Management's Response to the Draft Report

CHIEF
MISSION ASSURANCE

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

RECEIVED
SEP 15 2005

September 14, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – "Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected" (Audit #200520005)

Security on the part of State Tax Agencies (Agencies) that receive and use Federal tax returns and return information (FTI) to administer State taxing laws is of prime importance to the Internal Revenue Service. Mission Assurance & Security Services (MA&SS) continues the many years of practice to support the proactive posture of its Safeguard Office.

The Safeguard Office disseminates technical guidance to the Agencies in regards to the Federal Safeguards Requirements pursuant to Internal Revenue Code (IRC) Section 6103(p)(4). IRC § 6103 authorizes the disclosures of FTI to the Agencies, provided that they are compliant with the Federal Safeguards Requirements. The Safeguard Office actively monitors the Agencies to ensure their compliance by assessing their security measures utilized to protect the confidentiality of all FTI in their possession. Monitoring involves providing ongoing safeguards technical advice in regards to Fed/State initiatives, reviewing initial and annual reports from the Agencies, reviewing ad hoc requests in regards to a variety of Agency initiatives that would involve the use of FTI, and conducting on-site safeguard reviews to ensure compliance with policies, procedures and guidelines derived from IRC § 6103.

For the four audit report recommendations, we do not concur with recommendation #1, we partially concur with both recommendations #2 and #3, and we concur with recommendation #4. Our detailed responses to the audit recommendations are included in the attachment. If you have any questions, please contact me at (202) 622-8910 or Dr. Ellen Pieklo, Deputy Director, Certification Testing, Evaluation & Assessment at (585) 262-1185.

Attachment

Management Response to Draft Audit Report – Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Audit #200520005)

RECOMMENDATION # 1: The Chief, Mission Assurance and Security Services (MA&SS) should obtain a formal decision from the Office of Management and Budget (OMB) as to the application of the Federal Information Security Management Act (FISMA) computer security requirements for systems at State agencies that receive Federal tax information.

CORRECTIVE ACTION TO RECOMMENDATION #1:

We do not concur with the recommendation. Our reviews of the State agencies are governed by Title 26, U.S. Code, Section 6103(p)(4). As such, the States are required to protect Federal tax information (FTI) in accordance with the requirements of the U.S. Code as well as the policies and procedures outlined in Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*. Collectively, these information security requirements include computer security (i.e., physical and logical) controls designed to protect FTI from unauthorized access, use or disclosure. The Internal Revenue Service (IRS) Safeguards Office performs onsite assessments of State agency facilities to evaluate the security posture and operating effectiveness of such computer security controls. Some of these onsite assessments are funded by the fees collected from the State agencies that enforce child support and administer welfare benefits, as payment for receiving FTI records.

Currently, FISMA legislation and the applicable National Institute of Standards and Technology (NIST) standards are not mandated for the State agencies receiving FTI. Authorized agencies participate in the IRS data exchange program to facilitate their operations and mission processing requirements. Specifically, State agencies receive FTI from IRS to facilitate State and local programs (e.g., child support enforcement, taxes, and welfare benefits) funded, operated, owned and administered by the States, or on behalf of the States. Conversely, this program is not implemented for the benefit, aid or support of IRS. State agencies are not accessing, connecting to, or using IRS major information systems (i.e., major applications, general support systems) to collect, maintain, process, store or transmit this information for IRS, or on behalf of IRS. In addition, State agency systems are not classified, inventoried, categorized, operated or used as representative subsets of IRS information systems. IRS merely functions as an information broker to the State agencies. Additional background information explaining why the state agencies are not subject to FISMA is included in Appendix I.

In the event there are future changes in the legislation, the Chief, Mission Assurance and Security Services will work with internal staff and all entities involved to implement changes.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN: N/A

Management Response to Draft Audit Report – Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Audit #200520005)

RECOMMENDATION # 2: The Chief, Mission Assurance and Security Services (MA&SS) should, if States receiving Federal tax information are required to comply with the FISMA requirements, require States to submit more useful and in-depth self-assessments annually, using NIST Special Publication 800-53, with their Safeguard Activity Reports. These self-assessments should be used by the MA&SS organization to better focus the scope of its Safeguard Reviews, resulting in a more efficient use of resources. Additionally, as part of the oversight of entities receiving Federal tax information, the Chief, MA&SS, should require the States to submit Plans of Actions and Milestones to track corrective actions at the States and follow up on prior issues identified.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We partially concur with the recommendation. We agree that NIST Special Publication 800-53 provides clear guidance for management, operational, and technical controls and we are in the process of revising Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, to incorporate the recommended security controls described in this NIST document.

Currently the States are not subject to FISMA. As such, we have not required them to complete annual self-assessments based on NIST 800-26 or NIST 800-53 guidance. Our inclusion of this self-assessment in our Safeguards Program may necessitate revision to Title 26, U.S. Code, Section 6103(p)(4) to carry the FISMA mandate down to the State level and may put undue burden on the States due to resource and financial limitations. Implementation would also need to be orchestrated with certain Federal agencies and national organizations. Specifically, this would be the Department of Health and Human Services (HHS), the Office of Child Support Enforcement (OCSE) and the Federation of Tax Administrators (FTA). In addition to the HHS and OCSE oversight responsibilities of the States, these Federal Agencies, as well as FTA, enjoy significant Congressional influence and governmental jurisdiction.

If after additional discussion with internal legal staff and all entities involved, we determine that this is necessary, we will educate the States in advance of this new requirement for receiving FTI. It is critical that we develop workable solutions for protecting FTI that take into account both resource and financial impact, since many of the State agencies might be forced to opt out of the data exchange program. This would directly impact the partnering relationship IRS has built with the State agencies over the years.

In regards to the Plan of Actions and Milestones (POA&M), the Safeguards Office (Safeguards) will alter the process by which we track security weaknesses. Safeguards will use Plans of Actions and Milestones as part of the new process to better manage recommended corrective actions and to more readily identify program-level weaknesses as these relate to the IRS Safeguards Program.

IMPLEMENTATION DATE:

August 15, 2006

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN:

The Safeguard Office will develop an action plan to monitor POA&M implementation on a monthly basis.

Management Response to Draft Audit Report – Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Audit #200520005)

RECOMMENDATION # 3: The Chief, Mission Assurance and Security Services (MA&SS) should improve the scope of the IRS Safeguard Reviews by following NIST Special Publication 800-53 guidance.

CORRECTIVE ACTION TO RECOMMENDATION #3:

We partially concur with this recommendation. The Chief, MA&SS intends to incorporate NIST 800-53 recommended security controls for Federal information systems into the computer security safeguard review process for external agencies authorized to receive FTI. However, since the States are not subject to FISMA, OMB, or NIST guidance, it may not be practical to incorporate all of the recommended Federal security controls from NIST 800-53 into the Safeguard review methodology. Publication 1075 will be updated to incorporate the viable recommended security controls that are described in NIST Special Publication 800-53, allowing for some flexibility in the requirements imposed for the States as appropriate. The current assessment process, policies, procedures, presentations, and reporting format used to review and report agencies' practices in regards to FTI, will be updated in accordance with the revised Publication 1075 guidelines. Additionally, staff within the MA&SS organization will be trained and detailed to conduct Safeguard Reviews.

IMPLEMENTATION DATE:

October 15, 2008

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN:

The Safeguard Office will conduct briefings associated with the on-site Safeguard reviews to convey and clarify changes in computer security requirements prior to implementation. In addition, a letter will be sent from the Chief, Mission Assurance and Security Services to notify all agencies of the new guidance and allow the States an adequate period for compliance.

Management Response to Draft Audit Report – Increased IRS Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected (Audit #200520005)

RECOMMENDATION # 4: The Chief, Mission Assurance and Security Services (MA&SS) should assign more staffing to the MA&SS organization's Safeguards Program so adequate oversight can be provided to the States.

CORRECTIVE ACTION TO RECOMMENDATION #4:

We concur with this recommendation. The Chief MA&SS will review staffing proposals to determine the corresponding staffing needs for the additional workload items presented in this report.

In the interim, MA&SS personnel have been identified to assist in conducting the computer security reviews. We will continue to conduct computer security and safeguard training periodically as needed. The next training class is planned for April 2006.

IMPLEMENTATION DATE:

October 15, 2006

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN:

The Safeguard Office will present all staffing issues to the Chief, Mission Assurance and Security Services during our quarterly performance review.

Appendix I

The Safeguards Office has responsibility for ensuring state agencies authorized to receive FTI are adequately protecting the data, in accordance with the requirements of Internal Revenue Code (IRC) Section 6103(p)(4) and the policy and procedures requirements outlined in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. Authorized agencies participate in this data transfer program to facilitate their operations and mission processing requirements. Specifically, state agencies purchase FTI from IRS to facilitate state and local programs (e.g., child support enforcement, welfare) funded, operated, owned or administered by the states, or on behalf of the states. Conversely, this program is not implemented for the benefit, aid or support of IRS. State agencies are not accessing, connecting to, or using IRS major information systems (i.e., major applications, general support systems) to collect, maintain, process, store or transmit this information for IRS, or on behalf of IRS. IRS merely functions as an information broker to the state agencies. Furthermore, program oversight is subject to the information security provisions of IRC 6103(p)(4) and Publication 1075. Collectively, these information security requirements include computer security (i.e., physical and logical) controls designed to protect FTI from unauthorized access, use or disclosure. The IRS Safeguards Office performs onsite assessments of state agency facilities to evaluate the security posture and operating effectiveness of such computer security controls. These onsite assessments are funded by the fees collected from state agencies as payment for receiving FTI records.

We reviewed FISMA legislation (Subchapter III – Information Security, Chapter 35 of title 44, United States Code) and OMB's Frequently Asked Questions for FISMA Security Reporting (Questions 1-21, pgs 4-10) in efforts to interpret FISMA requirements and assess any probable impact or applicability to FTI provided to authorized state agencies as prescribed under the auspices of IRC 6103(p)(4). Our observations and interpretations of the respective, aforementioned documents are reflected in the tables below. The first table provides key excerpts from FISMA legislation, our interpretations of the legislation, and our rational conclusions associated with such interpretations:

No#	FISMA LEGISLATION	SAFEGUARDS COMMENT
1	Section 3544 - Federal agency responsibilities (a) In General. The head of each agency shall (1) be responsible for (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;	**Interpretation:** The head of each Federal executive agency (i.e., the term 'agency' as defined by section 3502(1) of title 44, United States Code) is responsible for providing sufficient levels of information security protection to mitigate the risk of unauthorized access, use, disclosure, disruption, modification, or destruction of: 1. Information collected by the Federal agency 2. Information collected on behalf of the Federal agency 3. Information maintained by the Federal agency 4. Information maintained on behalf of the Federal agency And; 1. Information systems operated by a Federal agency 2. Information systems operated by a contractor of a Federal

No#	FISMA LEGISLATION	SAFEGUARDS COMMENT
		agency 3. Information systems operated by other organization on behalf of a Federal agency **Conclusion:** Section 3544 appears to establish the essential crux, criteria or overarching conditions under which FISMA applies. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agencies are not contractors of IRS 2. State agencies do not collect information on behalf of IRS 3. State agencies do not maintain information on behalf of IRS 4. State agencies do not operate information systems on behalf of IRS
2	Section 3544 - Federal agency responsibilities (b) Agency Program. Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes: (4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency; (5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing (5A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);	**Interpretation:** Each Federal executive agency is responsible for developing, documenting and implementing an agencywide information security program to provide information security for information and information systems that support the operations and assets of the Federal agency. This oversight program also applies to the following information systems that support the operations and assets of the Federal agency: 1. Information systems provided by another agency, contractor, or other source 2. Information systems managed by another agency, contractor, or other source All information systems that support the operations and assets of the Federal agency shall be tested at least annually. Testing should include a review of management, operational and technical controls of every information system identified in the Federal agency's inventory of its major information systems, as required under section 3505(c) entitled "Inventory of Major Information Systems". Under section 3505(c), the inventory of major information systems includes those information systems operated by the Federal agency or under the control the Federal agency; and the interfaces between such information systems to other systems or networks (including those other systems or networks not operated by the Federal agency or under the control of the Federal agency). **Conclusion:** Section 3544 appears to establish the Federal agency's responsibility for implementing a security program to provide oversight of information and information systems that support the assets and operations of the Federal agency. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agencies do not receive, process or manage FTI to support the operations (i.e., mission) and assets of IRS 2. Information systems used or operated by state agencies are not used to support the operations and assets of IRS 3. Information systems used or operated by state agencies are not included in the IRS inventory of major information

No#	FISMA LEGISLATION	SAFEGUARDS COMMENT
		systems 4. Information systems and resources used, operated, owned or funded by state agencies are not (and should not) be factored into IRS budgeting, acquisition and information technology plans (to the extent such information systems are not used or operated by IRS or on behalf of IRS)
3	Section 3545 – Annual independent evaluation (a) In General. Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. (2) Each evaluation under this section shall include *(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;	**Interpretation:** At least annually, each Federal executive agency should perform an independent evaluation of its information security program and practices to determine the effectiveness of such program and practices. Each evaluation should include testing the operating effectiveness of information policies, procedures and practices applicable to a representative subset (e.g., population, sample, compartment, division, department) of the Federal agency's information systems. **Conclusion:** Section 3545 appears to focus exclusively on identifying the types of information systems subject to annual independent evaluations. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency information systems are not classified, inventoried, categorized, operated or used as representative subsets of IRS information systems 2. State agency information systems are not used or operated by or on behalf of IRS; and therefore, do not appear to qualify as IRS major information systems subject to annual independent evaluations
4	Section 11331 – Responsibilities for Federal information system standards (g) Definitions. In this section: *(1) Federal Information System. The term 'Federal information system' means an information system used or operated by an executive agency , by a contractor of an executive agency, or by another organization on behalf of an executive agency.	**Interpretation:** A federal information system is an information system: 1. Used or operated by a Federal executive agency 2. Used or operated by a contractor of an executive Federal agency 3. Used or operated by another organization on behalf of an executive Federal agency **Conclusion:** Section 11331 appears to clearly define the meaning of a Federal information system and identifies the National Institute of Standards & Technology (NIST) as the authoritative governing body responsible for developing and promulgating mandatory information security standards and guidelines pertaining to Federal information systems. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency information systems are not used, operated, classified or categorized as Federal information systems 2. State agency information systems are not operated or used by IRS 3. State agency information systems are not used or operated as contractor systems of IRS or on behalf of IRS

No#	FISMA LEGISLATION	SAFEGUARDS COMMENT
		4. NIST does not prescribe mandatory information security standards and guidelines for state agency information systems not used, operated, classified or categorized as Federal information systems.
5	Section 11331 – Responsibilities for Federal information system standards (b) Mandatory Requirements (1) Authority to Make Mandatory. Except as provided under paragraph [2], the Secretary shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary to improve efficiency of operation or security of Federal information systems.	**Interpretation:** The Secretary of Commerce shall make NIST standards and guidelines prescribed under subsection (a)(1) mandatory and binding to the extent necessary to improve efficiency in the operation of, or the security of, Federal information systems. **Conclusion:** Section 11331 appears to make applicable NIST standards and guidelines (i.e., associated with the NIST FISMA Implementation Project) mandatory for providing oversight and security of Federal information systems. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because state agency information systems are not operated, used, classified or categorized as Federal information systems (as defined in Section 11331 of title 40, United States Code).
6	Section 11331 – Responsibilities for Federal information system standards (e) Application of More Stringent Standards. The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision within of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards "(1) contain at least the applicable standards made compulsory and binding by the Secretary; and (2) are otherwise consistent with policies and guidelines issued under section 3543 of title 44".	**Interpretation:** The head of a Federal executive agency may deploy more stringent standards to protect Federal information systems within or under that Federal executive agency's control, as long as those standards are: 1.) (at a minimum) consistent with the applicable NIST standards made mandatory and binding by the Secretary of Commerce; and b.) otherwise consistent with the policies and guidelines prescribed under section 3543 of title 44. **Conclusion:** Section 11331 appears to permit Federal executive agencies to use more stringent information security standards to protect Federal information systems within or under the Federal executive agency's control. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency information systems are not used, operated, classified or categorized as Federal information systems (as defined in Section 11331 of title 40, United States Code) 2. State agency information systems are not used or operated within or under the supervision (i.e., control) of IRS
7	Section 11331 – Responsibilities for Federal information system standards (a) In General. The Institute shall "(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems……"	**Interpretation:** The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines (including minimum security requirements) for Federal information systems: 1. Used or operated by a Federal agency 2. Used or operated by a contractor of a Federal agency 3. Used or operated by another organization on behalf of a Federal agency **Conclusion:** Section 11331 appears to establish the responsibilities for NIST to develop and promulgate information

No#	FISMA LEGISLATION	SAFEGUARDS COMMENT
		security standards and guidelines for Federal information systems. Consequently, FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency information systems are not used, operated, classified or categorized as Federal information systems (as defined in Section 11331 of title 40, United States Code) 2. State agency information systems are not operated or used by IRS 3. State agency information systems are not used or operated as contractor systems of IRS or on behalf of IRS

The second table provides key excerpts from OMB's Frequently Asked Questions (FAQs), OMB responses to each FAQ, our interpretations of OMB's responses to each FAQ, and our conclusions associated with such interpretations:

No#	OMB FREQUENTLY ASKED QUESTIONS (FAQs)	SAFEGUARDS COMMENT
1	1. *What systems should be reported under FISMA?* FISMA applies to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. All systems meeting this definition shall be included in the report.	**Interpretation:** FISMA legislation applies to information systems used or operated by a Federal agency or by a contractor of a Federal agency or other organizations on behalf of (i.e., for, in support of, in aid of) a Federal agency. All information systems meeting this definition shall be included in the annual FISMA report. Conversely, information systems not meeting this definition shall not be included in the annual FISMA report. The term "information system" has the same meaning as the term "Federal information system" (as defined in Section 11331 of title 40, United States Code). **Conclusion**: FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency systems are not used or operated by IRS 2. State agencies are not IRS contractors 3. State agency systems are not contractor systems of IRS 4. State agency systems are not operated or used on behalf of IRS 5. State agency systems are not categorized or classified as Federal information systems (as defined in Section 11331 of title 40, United States Code).
2	6. *Do all agency systems have to be reviewed annually?* Yes. Senior agency program officials and CIOs must review all systems at least annually. Only the depth and breadth of such system reviews are flexible.	**Interpretation:** At least annually, Senior Federal agency program officials and CIOs must review all Federal agency systems under that Federal agency's respective control. Although these system reviews are mandatory under FISMA, the depth and breadth of such system reviews are flexible. **Conclusion:** FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agency information systems are not used, operated, identified, inventoried, or categorized as IRS information systems 2. State agency information systems are not used, operated or administered under the respective control or supervision of IRS
3	7. *What level of review is required for an individual system?* Program officials and CIOs are responsible for reviewing the security of all systems under their respective control. Clearly, the necessary depth and breadth of an annual system review depends on several factors such as: 1) the potential risk and magnitude of harm to the system and data; 2) the relative comprehensiveness of last year's review; and 3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation (consistent with NIST or national security	**Interpretation:** Federal agency program officials and CIOs are responsible for reviewing the security of all information systems under that Federal agency's respective control. The depth and breadth of an annual system review is flexible and primarily depends on the three factors cited. Program officials and CIOs must take these three factors into consideration in determining the appropriate level of annual system review. **Conclusion:** FISMA legislation does not appear to apply to state agencies participating in this program because:

No#	OMB FREQUENTLY ASKED QUESTIONS (FAQs)	SAFEGUARDS COMMENT
	guidance), this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented within the agency. An effective security program demands comprehensive and continuous understanding of program and system weaknesses. At a minimum, agency program officials and CIOs must take into account the three criteria listed above in determining the appropriate level of annual review IGs may report on the adequacy of such reviews.	1. State agency information systems are not used, operated, identified, inventoried, or categorized as IRS information systems 2. State agency information systems are not used, operated or administered under the respective control or supervision of IRS
4	14. *Must government contractors abide by FISMA requirements?* Yes. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing government information and interconnecting systems. Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems. Finally, because FISMA applies to Federal information (in addition to information systems), in certain limited circumstances its requirements also apply to a specific class of information technology to which Clinger-Cohen did not, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal information is used within incidentally acquired equipment, the agency is responsible for ensuring FISMA requirements are met.	**Interpretation:** Government contractors, using or operating information systems on behalf of a Federal agency, must comply with FISMA requirements. FISMA requires each Federal agency to provide information security for the information and information systems supporting the operations and assets of that Federal agency, including those information systems provided or managed by another agency, contractor, or other source. Specifically, Federal agency IT security program apply to all organizations (sources) which: 1.) possess of use Federal information on behalf of a Federal agency; or 2.) have access to Federal information systems on behalf of a Federal agency. These two factors succinctly define the essential application of FISMA requirements to those organizations using or operating information systems to support the operation and assets of a Federal agency. Within this context, such other organizations may include Federal agency contractors, state and local governments, and mission partners. Federal agencies must develop policies to provide oversight of contractors and other sources (users) with privileged access to Federal information and related Federal information systems. Federal agencies must also review the security of contractors and other sources (users) with privileged access to Federal information and related Federal information systems. **Conclusion:** FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agencies do not possess or use Federal information on behalf of IRS 2. State agencies do not operate, use, or have access to Federal information systems on behalf of IRS 3. State agencies are not IRS contractors 4. State agency information systems are not identified, inventoried, and categorized as Federal information systems (as defined in Section 11331 of title 40, United States Code
5	15. *Could you provide examples of IT acquired "incidental" to a contract and thus not subject to FISMA?* Again, in considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "…commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf	**Interpretation:** It is important to remember the specific, overarching context to which FISMA applies. FISMA requires Federal agencies to provide security protections for Federal information collected or maintained by or on behalf of a Federal agency; in addition to Federal information systems used or operated by a Federal agency or other organization on behalf of a Federal agency. For FISMA purposes, Federal information and

No#	OMB FREQUENTLY ASKED QUESTIONS (FAQs)	SAFEGUARDS COMMENT
	of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." A corporate human resource or financial management system acquired solely to assist managing corporate resources assigned to a government contract could be incidental, provided the system does not use agency information or interconnect with an agency system.	Federal information systems are not mutually exclusive components. Specifically, this Federal information refers to information processed, stored or transmitted by Federal information systems: 1.) used or operated by a Federal agency; or 2.) used or operated by organizations on behalf of a Federal agency. **Conclusion:** FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agencies do not collect or maintain Federal information on behalf of IRS 2. State agencies do not use or operate Federal information systems on behalf of IRS
6	16. *Could you provide examples of agency security responsibilities concerning contractors and other sources?* In considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." While we cannot anticipate all possible combinations and permutations, there are three primary categories of contractors as they relate to securing systems and information: 1) service providers, 2) contractor support, and 3) Government Owned Contractor Operated facilities (GOCO). 1) Service providers – this encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services. Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent" security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation must, at a minimum, explicitly meet guidance from NIST. Additionally, IGs shall include some contractor systems in their "representative subset of agency systems," and not doing so presents an incomplete independent evaluation. 2) Contractor support – this encompasses on or offsite contractor technical or other support staff. Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent" security procedures. Specifically, the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., general and	**Interpretation:** It is important to remember the specific, overarching context to which FISMA applies. FISMA requires Federal agencies to provide security protections for Federal information collected or maintained by or on behalf of a Federal agency; in addition to Federal information systems used or operated by a Federal agency or other organization on behalf of a Federal agency. Although OMB cannot anticipate all possible categories, there are three primary categories of contractors as they relate to securing Federal information systems and Federal information: 1) service providers, 2) contractor support, and 3) Government Owned Contractor Operated facilities (GOCO). Service providers includes outsourcers of system or network operations, telecommunications services, or other managed services. Contractor support includes onsite or offsite contractor technical or other support staff. For FISMA purposes, Government Owned, Contractor Operated (GOCO) facilities are Federal agency components. **Conclusion:** FISMA legislation does not appear to apply to state agencies participating in this program because: 1. State agencies are not IRS contractors 2. The "service provider" designation does not apply to State agencies 3. The "Contractor support" designation does not apply to State agencies 4. The "GOCO" designation does not apply to State agencies

No#	OMB FREQUENTLY ASKED QUESTIONS (FAQs)	SAFEGUARDS COMMENT
	specific). 3) Government Owned, Contractor Operated (GOCO) – For the purposes of FISMA, GOCO facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in terms of the contract.	

We also reviewed the following key FISMA guidance from NIST to determine if such standards and guidelines are mandatory for state agencies participating in this program:

- FIPS PUB 199 (Standards for Security Categorization of Federal Information and Information Systems)
- FIPS PUB 200 (Minimum Security Requirements for Federal Information and Information Systems)
- NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems)
- NIST SP 800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems)
- NIST SP 800-53 (Recommended Security Controls for Federal Information Systems)
- NIST SP 800-53A (Guide for Assessing Security Controls in Federal Information Systems)
- NIST SP 800-59 (Guideline for Identifying an Information System as a National Security System)
- NIST SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories)

In short, for FISMA purposes, we believe FIPS PUB 199 represents the key starting point in developing and implementing an enterprise risk management cycle for protecting information systems supporting the assets and operations of executive Federal agencies. According to NIST, FIPS PUB 199 is the essential "cornerstone" standard to be used by all Federal agencies in categorizing all information and information systems collected or maintained by, or on behalf of, each Federal agency based on the objectives of providing appropriate levels of information security according to impact. Specifically, this standard requires all Federal agencies to categorize their own information systems (i.e., general support systems, major applications) as low-impact, moderate-impact, or high-impact systems. Consequently, we believe the remaining NIST publications mentioned above were designed to fulfill FISMA compliance requirements by: 1.) accentuating the intent of FIPS PUB 199, and 2.) providing standards to facilitate security program oversight of information and information systems used or operated by a Federal agency, or on behalf of a Federal agency. Within this context, we conclude FISMA legislation and the applicable NIST standards are not mandated for the state agencies receiving Federal tax information under this program.