TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements

September 22, 2006

Reference Number: 2006-20-166

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

Phone Number | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 22, 2006

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

This report presents the results of our review to determine whether the Office of Privacy and Information Protection has effective controls and procedures to ensure Internal Revenue Service (IRS) computer systems and employees adhere to privacy regulations. This review was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2006 Annual Audit Plan and was part of the Information Systems Programs statutory requirements to annually review the adequacy and security of IRS technology.[1]

Impact on the Taxpayer

The IRS processes and maintains sensitive taxpayer information in computer systems for over 130 million taxpayers. Privacy Impact Assessments (PIA)[2] have not been conducted for all computer systems, and compliance with privacy laws has not been adequately monitored. As a result, the risk is increased that taxpayers' identities could be stolen and used for unlawful purposes.

---

[1] IRS Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

[2] A PIA is an analysis of how personal information is collected, stored, shared, and managed in a Federal Government system. Specifically, a PIA (1) ensures handling conforms to applicable legal, regulatory, and policy requirements on privacy; (2) determines the risks and effect of collecting, maintaining, and disseminating personal information; and (3) examines and evaluates protection and alternative processes for handling personal data to reduce potential privacy risks.

Synopsis

The issue of privacy and security over personal information has received much publicity. For example, the Department of Veterans Affairs[3] recently reported that personally identifying data for as many as 26 million American veterans were stolen from an employee's home. This incident received significant attention because the loss of personally identifying data can represent the first step to identity theft. In 2004, the IRS received more than 130 million individual taxpayers' income tax returns. The personal information contained in these returns is converted into electronic format and used in over 240 IRS computer systems.

The IRS is not complying with privacy legislation. As a result, the IRS does not have assurance that privacy implications have been considered and evaluated on all of its computer systems.

Within the past 2 years, the Office of Privacy and Information Protection[4] has maintained and enhanced the IRS' privacy program by chairing a working group reviewing privacy and disclosure issues and by creating an online privacy training segment on the Office of Privacy and Information Protection web site. Despite these efforts, the IRS is not complying with legislative privacy requirements. Specifically, the IRS can take further actions to ensure PIAs have been conducted for all systems and applications that collect personal information and enhance its processes to better monitor compliance with privacy policy and procedures.

The E-Government Act of 2002[5] and IRS guidelines require every computer system or project that collects personal information to have a current PIA on file with the Office of Privacy and Information Protection. As of August 2005, we were unable to locate PIAs for 130 (54 percent) of the 241 IRS computers systems that collect and process taxpayer or employee data. We attribute the missing PIAs to the lack of emphasis on privacy issues and the decision to not require that all systems be certified and accredited.[6]

Also, the PIA review process was not always consistently conducted, and review results were not always properly documented. At the time the Office of Privacy and Information Protection

---

[3] The Department of Veterans Affairs provides patient care, veterans' benefits, and customer satisfaction for our nation's veterans and their families.

[4] The administration of the IRS' privacy program is the responsibility of the Director, Office of Privacy and Information Protection, who reports to the Chief, Mission Assurance and Security Services. The mission of the Office of Privacy and Information Protection is to ensure IRS policies and programs incorporate taxpayer and employee privacy requirements and the personal information entrusted to the IRS remains protected, secure, and private.

[5] Pub. L. No. 107-347 (2002), sec. 208.

[6] Certification and accreditation, as defined and required by the Office of Management and Budget for all Federal Government automated information systems, is a process to provide assurance that adequate security controls are in place over computer systems.

completed the PIAs, there were no PIA review procedures and no core list of source information to verify system facts and information. As a result, PIA reviews were not consistently performed. The analysts did not properly document actions pending or taken in a history log and can review the answers provided in the PIA only for consistency.

In addition, the Office of Privacy and Information Protection did not conduct any compliance reviews on existing PIAs. IRS procedures provide for compliance reviews as a means to validate that information submitted in the PIA truly represents the data being collected in the computer system or project. These compliance reviews can provide opportunities to update and verify information stated in the PIAs and ensure business units are complying with privacy policies and procedures.

By addressing these areas, the Office of Privacy and Information Protection would better fulfill its responsibility to create and maintain privacy awareness and monitor all uses of taxpayer data by IRS employees. This will provide the first steps to ensure the security and protection over taxpayer data throughout the agency.

Recommendations

We recommended the Chief, Mission Assurance and Security Services, request business owners to identify and report all systems or projects that collect personal identifiable information. A PIA should be prepared and submitted to the Office of Privacy and Information Protection for monitoring, oversight, and evaluation. The Director, Office of Privacy and Information Protection, should establish a centralized repository for all PIAs in a searchable, electronic format and verify the accuracy of the PIA inventory quarterly; initiate a program providing for the routine evaluation of employee training activities relative to current privacy policy requirements and develop a system for the tracking and monitoring of these activities; and reinforce the importance of PIA case documentation with specific instructions and implement a compliance review process to assess whether IRS business units are adhering to privacy regulations.

Response

The Chief, Mission Assurance and Security Services, agreed with our findings and recommendations. The Office of Privacy and Information Protection will annually cross-walk (reconcile) the PIA inventory to existing system inventories and provide information to business owners for systems requiring PIAs. The Office of Privacy and Information Protection will also develop and implement a process to verify the PIA inventory accuracy quarterly and is developing an electronic PIA inventory and an electronic document management system for archiving electronic PIA artifacts. In addition, the Office of Privacy and Information Protection is establishing privacy awareness training via the mandatory IRS Information Protection training

and will initiate a job-specific training program for privacy. Training will be deployed via the IRS Enterprise Learning Management System to ensure accurate monitoring and tracking. Finally, the Office of Privacy and Information Protection will establish assessment standards for PIAs to ensure consistency and extent of coverage based on system complexity, along with case documentation and analysis requirements. Management's complete response to the draft report is included as Appendix IV.

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

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

The Office of Privacy and Information Protection Needs to Ensure Required Privacy Impact Assessments Are Conducted and Tracked ..... Page 4

Recommendation 1: ..... Page 7

Recommendation 2: ..... Page 8

Monitoring of Privacy Compliance Can Be Enhanced ..... Page 8

Recommendations 3 and 4: ..... Page 11

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 13

Appendix II – Major Contributors to This Report ..... Page 15

Appendix III – Report Distribution List ..... Page 16

Appendix IV – Management's Response to the Draft Report ..... Page 17

Abbreviations

FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
PIA	Privacy Impact Assessment

Background

Within the Federal Government, privacy can be defined as a citizen's expectation that personal information collected for official Government business will be protected from unauthorized use and access. The issue of privacy and security over personal information has received much publicity since 2005. For example, in February 2005, the Bank of America reported the loss of data tapes that contained personal information on 1.2 million Federal Government employees. More recently, in May 2006, the Department of Veterans Affairs[1] reported that personally identifying data for as many as 26 million American veterans were stolen from an employee's home. These incidents received significant attention because the loss of personally identifying data can represent the first step to identity theft, which occurs when someone uses personal information, without permission, to commit fraud or other crimes, such as opening fraudulent credit card accounts and purchasing goods.

The Federal Trade Commission[2] has reported increased filings of identity theft complaints, and the Privacy Rights Clearinghouse[3] estimates that, during 2005, over 50 million people had been put at risk as a result of security breaches. The average identity theft victim spends 175 hours and $800 resolving identity theft-related issues, and it takes 2 years to 4 years for victims to resolve all the resulting problems.

Like the private sector, the Federal Government collects enormous amounts of personal information from private citizens. For example, in 2004 the Internal Revenue Service (IRS) received more than 130 million individual taxpayers' income tax returns. Each of these tax returns includes the filer's name, address, Social Security Number, and other personal financial data. This personal information is

The mission of the IRS Office of Privacy and Information Protection is to ensure IRS policies and programs incorporate taxpayer and employee privacy requirements, and the personal information entrusted to the IRS remains protected, secure, and private.

[1] The Department of Veterans Affairs provides patient care, veterans' benefits, and customer satisfaction for our nation's veterans and their families.
[2] The Federal Trade Commission was created in 1914 to prevent unfair methods of competition in commerce and to police anticompetitive practices.
[3] The Privacy Rights Clearinghouse is a nonprofit consumer organization established to raise consumer awareness of how technology affects personal privacy, empower consumers to take action to control their own personal information by providing practical tips on privacy protection, and respond to and document specific privacy-related complaints from consumers.

converted into electronic format and used in over 240 IRS computer systems, such as the Integrated Data Retrieval System.[4]

From a legislative perspective, the issue of privacy is governed by several laws. The Privacy Act of 1974[5] placed limitations on Federal Government agencies' collection, disclosure, and use of personal information maintained in computer systems. More recently, the E-Government Act of 2002[6] provided additional protection for personal information by requiring agencies to conduct Privacy Impact Assessments (PIA). A PIA is required for every computer system or project that collects personal information and must be maintained by the bureaus and agencies. A PIA represents an analysis of how personal information is handled to ensure it conforms to applicable legal and regulatory requirements over privacy; determines the risks and effects of collecting, maintaining, and disseminating information in identifiable form; and examines and evaluates protections and alternative processes for handling information to reduce potential privacy risks. Systems must be reevaluated every 3 years or when major system modifications[7] occur.

In addition, the Consolidated Appropriations Act of 2005, Section 522,[8] required each agency to have a Chief Privacy Officer to assume the responsibility for privacy and data protection policy. These legislative requirements provide the need for a strong privacy program within Federal Government bureaus and agencies.

The administration of the IRS privacy program is the responsibility of the Director, Office of Privacy and Information Protection, who reports directly to the Chief, Mission Assurance and Security Services. The mission of the Office of Privacy and Information Protection is to ensure IRS policies and programs incorporate taxpayer and employee privacy requirements and the personal information entrusted to the IRS remains protected, secure, and private.

This review was performed at the IRS National Headquarters in Washington, D.C., in the Office of Privacy and Information Protection during the period September 2005 through March 2006. 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.

[4] This is an IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[5] 5 U.S.C. § 552a (a)(5).
[6] Pub. L. No. 107-347 (2002), sec. 208.
[7] A major modification is any programming or equipment change that affects how the system interfaces with users, processes data, or generates reports. In addition, these changes may affect the security of the system.
[8] Pub. L. No. 108-447, 188 Stat. 2268, 5 U.S.C. 522a note.

Results of Review

Because of the large amount of personal information it receives and concern over privacy implications of maintaining that information, the IRS established the Privacy Advocate position in 1993, becoming the first Federal Government agency to assign privacy to an executive official. Within the past 2 years, the Office of Privacy and Information Protection has maintained and enhanced the IRS' privacy program by:

- Chairing a working group reviewing privacy and disclosure issues to be included in the IRS annual security training, as well as serving as a member of several inter- and intra-agency committees and task groups.
- Increasing privacy awareness by having the Office of Privacy and Information Protection actively participate in the IRS' annual Security Awareness week in the National Headquarters Office.
- Updating and distributing privacy literature to IRS security managers and records officers and to over 70,000 volunteer tax preparers through Volunteer Income Tax Assistance[9] and Tax Counseling for the Elderly[10] Centers.
- Creating an online privacy training segment on the Office of Privacy and Information Protection web site.

Despite the Office of Privacy and Information Protection's efforts to increase privacy awareness and manage its program, the IRS is not complying with legislative privacy requirements and, thus, is not ensuring the privacy of taxpayer data is being tracked and monitored adequately. Specifically, the IRS can take further actions to ensure PIAs have been conducted for all systems and applications that collect personal information and enhance its processes to better monitor compliance with privacy

The IRS can take further actions to ensure PIAs have been conducted for all systems that collect personal information and enhance its processes to better monitor compliance with privacy policy procedures.

[9] The Volunteer Income Tax Assistance Program offers free tax help for low- to moderate-income (approximately $38,000) people who cannot prepare their own tax returns. Volunteers, sponsored by various organizations, receive training to help prepare basic tax returns in communities across the country. Volunteer Income Tax Assistance sites are generally located at community and neighborhood centers, libraries, schools, shopping malls, and other convenient locations. Some locations also offer free electronic filing.

[10] The Tax Counseling for the Elderly Program provides free tax help to people age 60 and older. Trained volunteers from nonprofit organizations provide free tax counseling and basic income tax return preparation for senior citizens. Volunteers who provide tax counseling are often retired individuals associated with nonprofit organizations that receive grants from the IRS.

policy and procedures. These improvements will allow the IRS to better identify and monitor all uses of taxpayer data and will provide the first steps to ensure the security and protection over taxpayer data throughout the agency.

The Office of Privacy and Information Protection Needs to Ensure Required Privacy Impact Assessments Are Conducted and Tracked

Computer systems that collect personal information did not have PIAs

The E-Government Act of 2002 and IRS guidelines require every computer system or project that collects personal information to have a current PIA on file with the Office of Privacy and Information Protection. The existence of the PIA provides reasonable assurance that privacy implications have been considered and evaluated in the collection of the data. Systems must be reevaluated every 3 years.

As of August 2005, the IRS maintained 281 computer systems to assist in tax administration. Of these, 241 collected and processed personal information, consisting of either taxpayer or employee data. Based on privacy requirements, each of these 241 systems should have a PIA completed by system owners and maintained by the Office of Privacy and Information Protection. However, we were unable to locate PIAs for 130 (54 percent) of the 241 computer systems.

The IRS classifies its computer systems into three categories: general support systems, major applications, and nonmajor applications.[11] Table 1 presents the number of computer systems in each classification that did not have a PIA.

[11] A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A major application is a computer system that requires special management oversight because of the information it contains, processes, or transmits or because of its criticality to the organization's mission. A nonmajor application is a computer system that does not require special management oversight because the information it contains, processes, or transmits is less critical to the organization's mission.

Table 1: Number of Computer Systems Without PIAs That Collect Taxpayer or Employee Data

System Classification	Total Number of Computer Systems	Number of Computer Systems That Process or Collect Personally Identifiable Data	Number of Computer Systems Without a Required PIA Statement
General Support Systems	29	29	21 (72%)
Major Applications	53	53	5 (9%)
Nonmajor Applications	199	159	104 (65%)
Totals	281	241	130 (54%)

Source: The Office of Privacy and Information Protection's inventory lists and our report entitled Treasury Inspector General for Tax Administration - Federal Information Security Management Act Report for Fiscal Year 2005 (Reference Number 2006-20-071, dated October 2005).

We attribute the missing PIAs to the lack of emphasis on privacy issues and the decision to not require that all systems be certified and accredited,[12] which included the submission of PIAs as part of the certification process.

- We believe the IRS did not maintain an emphasis on the importance of privacy prior to the arrival of the current Director, Office of Privacy and Information Protection, in April 2005. The Office of Privacy and Information Protection has had three different Directors and several acting officials since 2003 and has encountered several organizational changes; the latest was in 2005 when it moved from directly reporting to the Deputy Commissioner for Operations Support to the Chief, Mission Assurance and Security Services. This lack of a permanent Director and organizational shuffling has not provided leadership continuity and organizational stability to the Office of Privacy and Information Protection and, as a result, has not allowed the importance of privacy to remain in the forefront within the IRS. In addition, the current Office of Privacy and Information Protection is authorized only 10 Full-Time Equivalent[13] employee positions,

[12] Certification is the comprehensive evaluation of the technical and nontechnical security controls and the identification of any weaknesses with those controls or lack thereof. Accreditation is an authorization granted by a management official to operate the system based on the evaluation of the security controls. It is a statement that the management official (i.e., the accrediting official) is aware of, understands, and accepts responsibility for the risks associated with placing the system into operation. Certification and accreditation, as defined and required by the Office of Management and Budget for all Federal Government automated information systems, is a process to provide assurance that adequate security controls are in place over computer systems.

[13] A Full-Time Equivalent is a measure of labor hours in which 1 Full-Time Equivalent is equal to 8 hours multiplied by the number of compensable days in a particular fiscal year.

which consist of 1 Director, 1 Deputy Director (currently vacant), 1 staff assistant, and 7 staff analysts (1 currently vacant), to implement its mission and oversee privacy within the IRS, an organization of over 100,000 employees.

- In 2005, the Office of Mission Assurance and Security Services assigned all of its nonmajor applications to 1 of the 29 general support systems. The rationale for this classification was that the general support systems would provide the majority of the security controls for the nonmajor applications. As such, the IRS placed less emphasis on documenting security and privacy requirements for the nonmajor applications, which included the completion of certification and accreditation. The certification process includes the submission of PIAs. This decision appears to explain why we were unable to locate PIAs for 65 percent of the nonmajor applications.[14]

The Office of Privacy and Information Protection, as part of its own poststudy review of the Federal Information Security Management Act (FISMA)[15] reporting process, found that "mapping the Office of Privacy and Information Protection inventory to the Fiscal Year 2005 FISMA inventory was difficult due to the inability to clearly identify the subcomponents of the general support systems and major applications." The Office of Privacy and Information Protection has acknowledged the lack of PIAs as a weakness and has taken proactive steps to increase privacy awareness, such as conducting awareness presentations to IRS business unit executives and in the IRS' annual Security Awareness week in the National Headquarters Office on the risks and requirements of privacy for computer systems maintaining personal identifiable information.

We believe it is critical that the IRS complete PIAs for all computer systems or projects in which personal information is collected, processed, used, and/or stored. When PIAs are not prepared and properly maintained, the IRS is unaware of all instances in which the collection of data is occurring, and the IRS could be violating privacy regulations and unnecessarily exposing sensitive data to theft or misuse. As such, public trust could be lost when privacy risks are not identified and privacy protections are not adhered to.

An effective management information system to track PIAs does not exist

The Office of Privacy and Information Protection recognizes that sound business practice requires a functional and useful centralized management information system to track and monitor its PIAs. The Office of Privacy and Information Protection is currently using a system

[14] The IRS has recently changed this requirement and decided to require certification and accreditation for all systems, regardless of classification, for Fiscal Year 2006.
[15] The FISMA is part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301 (2002). The FISMA includes protecting information and information systems from unauthorized access, use, disclosure, or modification, including controls for disclosure and confidentiality to protect personal privacy.

developed by the Office of Disclosure.[16] This system contains pre-set data fields and cannot be customized to add more useful information, so it is mainly used to assign and generate PIA control numbers. Because of this limitation, the Office of Privacy and Information Protection created two additional inventory systems to capture specific information for different uses. One system is used to calculate the number of days the PIA is open and when a recertification is due, and the second system is a working file for the analysts. Inefficiencies exist when the staff need to query two inventory lists to obtain basic information, such as the system name and associated PIA control number. Also, maintaining multiple inventory lists creates data inaccuracies, such as determining when a recertification of a system's PIA is due. For example, we identified the following discrepancies among the several PIA lists:

- There were 91 computer systems listed as recertified that had different PIA completion dates on each of the 3 lists.
- There were 20 computer systems listed as either "Retire" or "Dead"[17] on 1 list but shown as recertified on another list.

The Office of Privacy and Information Protection has also identified its management information system as a weakness in its poststudy review of the FISMA reporting process. As a result, the Office of Privacy and Information Protection is developing an electronic, menu-driven, and more user-friendly version of the PIA and has plans to incorporate and implement the new PIA in a new management information system scheduled to be completed by the end of Fiscal Year 2006.

Recommendations

Recommendation 1: The Chief, Mission Assurance and Security Services, should request IRS business owners to identify and report all systems or projects that collect personal identifiable information. A PIA should be prepared and submitted to the Office of Privacy and Information Protection for monitoring, oversight, and evaluation.

> ***Management's Response:*** IRS management agreed with this recommendation. The Office of Privacy and Information Protection will annually cross-walk (reconcile) the PIA inventory to existing system inventories and provide information to business owners for systems requiring PIAs. The Office of Privacy and Information Protection will also conduct a study to identify PIA process improvements to ensure limited resources are focused on systems that collect personal identifiable information and will establish policy, based on the study, for systems that require a PIA.

[16] The Office of Disclosure reports to the Director, Communications, Liaison, and Disclosure, within the Small Business/Self-Employed Division. The Office of Privacy and Information Protection reported to the Office of Disclosure from 2000 until 2003.

[17] Retired and dead computer systems are those no longer in use and no longer processing data for tax administration.

Recommendation 2: The Director, Office of Privacy and Information Protection, should establish a centralized repository for all PIAs in a searchable, electronic format. The process should be developed to verify the accuracy of the PIA inventory quarterly. The Office of Privacy and Information Protection should also develop an electronic document management system for archiving electronic PIA artifacts.

> ***Management's Response:*** IRS management agreed with this recommendation. The Office of Privacy and Information Protection will develop and implement a process to verify the PIA inventory accuracy quarterly. The Office of Privacy and Information Protection is also developing an electronic PIA inventory and an electronic document management system for archiving electronic PIA artifacts.

Monitoring of Privacy Compliance Can Be Enhanced

The Office of Privacy and Information Protection's role in the organization is to ensure the IRS is complying with privacy requirements. The E-Government Act established that the primary control over privacy compliance for the Federal Government is the use of PIAs. While the main goal should be to have complete and accurate PIAs for all instances in which the IRS is collecting and using sensitive data (i.e., taxpayer or employee data), equally important are the processes to ensure PIAs are being properly and accurately completed. Compliance with privacy requirements can be segmented into three key activities:

1. Providing awareness training to IRS employees on the privacy of taxpayer data requirements and on the completion of PIAs for all instances in which sensitive data are being collected.
2. Conducting initial reviews of submitted PIAs for completeness, accuracy, and consistency with IRS requirements.
3. Conducting compliance reviews of existing PIAs to validate adherences to information submitted in the PIAs.

We assessed the Office of Privacy and Information Protection's efforts in these three areas and determined it did not have a formal privacy training program, initial reviews of PIAs could be enhanced and better documented, and compliance reviews of PIAs were not conducted. By addressing these areas, the Office of Privacy and Information Protection would better fulfill its responsibility to create and maintain privacy awareness among IRS employees and monitor compliance with privacy requirements for the IRS as a whole.

The Office of Privacy and Information Protection does not have a formal training program

In an effort to help identify systems collecting personal information and increase awareness and compliance with privacy requirements, the Office of Privacy and Information Protection

conducts ad hoc training and awareness presentations whenever the opportunity arises. For example, the Director, Office of Privacy and Information Protection, and senior staff are members of task forces, committees, and professional organizations and have provided privacy expertise and privacy-related presentations at various meetings. This includes proactively giving awareness presentations to IRS business unit executives on the risks and requirements of privacy for computer systems maintaining personal identifiable information and collaborating with other IRS business units and the Department of the Treasury on proposed revisions to tax laws and implementation of a Department-wide PIA initiative. The Office of Privacy and Information Protection also developed an online, self-study privacy awareness segment that is available to all IRS employees. However, the Office of Privacy and Information Protection does not have a regular awareness training schedule or specific role-based privacy training, nor does it mandate the completion of its online, self-study privacy awareness training by all employees.

In addition, the Office of Privacy and Information Protection does not have a formal management information system to track training delivered to IRS employees. The Office of Privacy and Information Protection was unable to provide such basic information as the number of IRS employees and contractors who attended privacy-related training courses and awareness presentations, training costs expended, or staff days applied toward training. Due to our review, the Office of Privacy and Information Protection recently requested IRS employees who have completed the online, self-study privacy awareness training on the Office of Privacy and Information Protection's web site to send copies of their certificates of completion for tracking and documentation purposes. The Office of Privacy and Information Protection stated that, due to limited resources and staffing, a management information system to track privacy will be a long-range goal. The Director, Office of Privacy and Information Protection, is also working to develop a computer-based module to be included as part of the mandatory computer security and Unauthorized Access training.[18]

Without a formal training program and an effective tracking system, the Office of Privacy and Information Protection cannot be assured it is meeting its mission to inform, educate, and make all IRS employees aware of important privacy issues, policies, and requirements.

The PIA review process needs to be improved, and review documentation requirements need to be strengthened

Our analysis of a sample of 20 PIAs determined the PIA review process was not always consistently conducted and review results were not always properly documented. The 20 PIAs were conducted from November 2002 to September 2005. Specifically:

[18] Unauthorized Access training is an annual requirement for all IRS employees as a result of the Taxpayer Browsing Act of 1997, 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).

- Nine of the 20 PIAs were cursory and the information provided was taken at face value, especially for current production environment systems[19] for which supporting information may not be available or does not exist.
- Eleven of the 20 PIAs were lacking case history information and supporting documentation for statements made in the PIA, which, at a minimum, should be included in the case file. Most case files had comments or concerns made on the initial version of the PIA, but there were no indications as to the response or resolution of the comments or concerns. Generally, there was no case history information, which, if available, could be used by the Office of Privacy and Information Protection to better manage the privacy program through internal reviews and to determine whether further actions are needed or reasons for delays.
- Six of the 20 PIAs were to recertify an existing system. A simple, one-page form was used to recertify a PIA, but there was no supporting documentation or history log to indicate whether an indepth analysis was conducted to support the recertification or to verify the system had no "significant changes" subsequent to when the original PIA was prepared.

At the time the Office of Privacy and Information Protection completed the PIAs, there were no PIA review procedures, nor was there an available core list of source information to verify system facts and information. As a result, PIA reviews were not consistently performed. The analysts did not properly document actions pending or taken in a history log and can review the answers provided in the PIA only for consistency.

This issue was also reported by the Government Accountability Office.[20] The report cited the lack of a comprehensive assessment over an IRS system selected for review by not analyzing how the agency reached its decision in its response to a PIA question. The report stated that the IRS did not fully address these steps because it used a prior version of the guidance issued by the Office of Management and Budget.

Continued implementation of PIA review procedures would allow the Office of Privacy and Information Protection to (1) maintain a consistent quality of work and protect the IRS from violations of privacy regulations and statutes by identifying risks in the system and (2) limit information collection.

[19] These are computer systems currently in use and processing data for tax administration.
[20] *Data Mining, Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain* (GAO 05-866, dated August 2005).

The Office of Privacy and Information Protection did not conduct compliance reviews

Based on discussions with Office of Privacy and Information Protection personnel, we determined the Office of Privacy and Information Protection did not conduct any compliance reviews on existing PIAs. IRS procedures provide for compliance reviews as a means to validate that information submitted in a PIA truly represents the data being collected in the computer system or project. These compliance reviews can provide opportunities to update and verify information stated in the PIAs and ensure business units are complying with privacy policies and procedures. Compliance reviews also allow the Office of Privacy and Information Protection to have visibility within the IRS and to spread the importance of privacy throughout the agency.

The Office of Privacy and Information Protection recognizes the lack of compliance reviews as a deficiency, and the Director hopes to redirect limited resources and staffing in the Fiscal Year 2006 Business Plan to address and implement this plan of action. As mentioned above, implementation of these procedures would allow the Office of Privacy and Information Protection to maintain a consistent quality of work and better manage the privacy program.

Recommendations

Recommendation 3: To monitor employee privacy awareness training, the Director, Office of Privacy and Information Protection, should initiate a program providing for the routine evaluation of employee training activities relative to current privacy policy requirements and develop a system for the tracking and monitoring of these activities.

> ***Management's Response:*** IRS management agreed with this recommendation. The Office of Privacy and Information Protection is establishing privacy awareness training via the mandatory IRS Information Protection training. Also, the Office of Privacy and Information Protection will conduct an assessment of roles for which training must be given and initiate a job-specific training program for privacy. In addition, training modules on IRS privacy products, such as the PIA, will be developed. Training will be deployed via the IRS Enterprise Learning Management System to ensure accurate monitoring and tracking. To supplement the training, the Office of Privacy and Information Protection will develop and deploy an assessment methodology to survey IRS employees annually of their knowledge of privacy policy requirements, which will provide feedback on employee awareness and training needs.

Recommendation 4: The Director, Office of Privacy and Information Protection, should reinforce the importance of PIA case documentation with specific instructions or case models and implement a compliance review process to assess whether IRS business units are adhering to privacy regulations, given the limited resources and staff knowledge in conducting these reviews.

Management's Response: IRS management agreed with this recommendation. The Office of Privacy and Information Protection will establish assessment standards for PIAs to ensure consistency and extent of coverage based on system complexity, along with case documentation and analysis requirements. For the short term, the Office of Privacy and Information Protection will investigate tools, conduct a pilot of selected tools, assess results, and implement interim measures to establish and implement compliance review guidelines and a process to ensure adherence to privacy regulations. For the long term, the Office of Privacy and Information Protection will build on knowledge obtained in the short term and implement comprehensive measures to establish and implement compliance review guidelines and processes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Office of Privacy and Information Protection[1] has effective controls and procedures to ensure IRS computer systems and employees adhere to privacy regulations. To accomplish this objective, we:

I. Determined whether Office of Privacy and Information Protection controls and procedures were in place to ensure adherence to privacy regulations.

A. Determined whether a management information system was in place to track PIAs,[2] evaluated the type of data captured by the system, and obtained a list of all PIAs conducted to determine whether all systems in the IRS had a description of the information being maintained from a privacy perspective.

B. Selected and reviewed a representative judgmental sample of 20 of the 241 IRS systems that collect and process either taxpayer or employee personal information. We validated selected information from the PIAs to determine whether responses were accurate and adequately supported by documentation. We used a judgmental sample because we did not plan to project our results to the population and had received agreement to our conclusions after we completed our review of the 20 PIAs.

C. Obtained a list of privacy training classes and awareness presentations conducted since October 2003, determined whether a management information system was in place to track training sessions, and evaluated the type of data captured.

D. Evaluated the Fiscal Year 2005 and 2006 Business Plans for the Office of Privacy and Information Protection to determine whether plans and goals were included to promote employee and contractor privacy responsibilities, promote the mission and activities of the Office of Privacy and Information Protection, and make all employees and contractors aware of relevant privacy laws and policies.

[1] The administration of the IRS' privacy program is the responsibility of the Director, Office of Privacy and Information Protection, who reports to the Chief, Mission Assurance and Security Services. The mission of the Office of Privacy and Information Protection is to ensure IRS policies and programs incorporate taxpayer and employee privacy requirements and the personal information entrusted to the IRS remains protected, secure, and private.

[2] A PIA is an analysis of how personal information is collected, stored, shared, and managed in a Federal Government system. Specifically, a PIA (1) ensures handling conforms to applicable legal, regulatory, and policy requirements on privacy; (2) determines the risks and effect of collecting, maintaining, and disseminating personal information; and (3) examines and evaluates protection and alternative processes for handling personal data to reduce potential privacy risks.

E. Ascertained whether the Office of Privacy and Information Protection conducts compliance or "safeguard" reviews.

F. For the PIAs sampled in Step I.B, interviewed the business owner, program manager, and system administrator of the computer system to determine whether they had attended a privacy training class or awareness presentation within the past 2 calendar years; completed the online privacy training session available on the Office of Privacy and Information Protection web site; and coordinated adequately with the Office of Privacy and Information Protection, Office of Disclosure, and Office of Security.

G. Obtained from the Treasury Inspector General for Tax Administration Office of Investigations and the IRS Office of Disclosure a list of all instances of unauthorized and inadvertent disclosure of sensitive information. We evaluated whether a management information system was in place to track unauthorized disclosures and the type of data captured by the system.

II. Determined whether all programs (systems and research projects) collecting personally identifiable data had PIAs.

A. Met with Office of Privacy and Information Protection staff to determine their interpretation of the Consolidated Appropriation Act,[3] as it applies to "programs collecting personally identifiable data."

B. Obtained and reviewed the IRS inventory of computer systems included in our report entitled *Treasury Inspector General for Tax Administration - Federal Information Security Management Act Report for Fiscal Year 2005* (Reference Number 2006-20-071, dated October 2005) to identify systems that meet the definition of a "program collecting personally identifiable data" but did not have PIAs.

C. Obtained the Office of Privacy and Information Protection documentation supporting its responses to Section D (Reporting Template for Senior Agency Officials for Privacy) of the FISMA Reporting for Fiscal Year 2005 and reviewed the documentation to validate the accuracy of its "cross-walk" (reconciliation) of PIAs to the IRS inventory of computer systems.

D. Met with Office of Privacy and Information Protection personnel to discuss whether research projects meet the definition of "programs collecting personally identifiable data" that would require a PIA, particularly those conducted by the Office of Research or the Office of Statistics of Income.

[3] Pub. L. No. 108-447, 188 Stat. 2268, 5 U.S.C. 522a note.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Kent Sagara, Acting Director
Joseph Cooney, Acting Audit Manager
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Jackie Nguyen, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Commissioner, Small Business/Self-Employed Division SE:S
Acting Chief Information Officer OS:CIO
Director, Communications, Liaison, and Disclosure, Small Business/Self-Employed Division SE:S:CLD
Director, Office of Privacy and Information Protection OS:MA:OPIP
Director, Governmental Liaison and Disclosure, Small Business/Self-Employed Division SE:S:CLD:GLD
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Commissioner, Small Business/Self-Employed Division SE:S
- Acting Chief Information Officer: OS:CIO
- Chief, Mission Assurance and Security Services: OS:MA

Appendix IV

Management's Response to the Draft Report

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

CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

RECEIVED
SEP 13 2006

SEP 13 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit #200620002)

Thank you for the opportunity to review the subject draft audit report, dated August 15, 2006. The issue of privacy and security over personal information is a top priority for the IRS. We are pleased that your report details that the IRS established the Privacy Advocate position in 1993, becoming the first Federal Government agency to assign privacy to an Executive official. We also appreciate that the report acknowledges that within the past 2 years, the Office of Privacy and Information Protection has maintained and enhanced the IRS' privacy program by:

- Chairing a working group reviewing privacy and disclosure issues to be included in the IRS annual security training, as well as serving as a member of several inter- and intra-agency committees and task groups.
- Increasing privacy awareness by having the Office of Privacy and Information Protection actively participate in the IRS' annual Security Awareness week in the National Headquarters Office.
- Updating and distributing privacy literature to IRS security managers and records officers and to over 70,000 volunteer tax preparers through the Volunteer Income Tax Assistance Program and Tax Counseling for the Elderly Centers Program.
- Creating an online privacy training segment on the Office of Privacy and Information Protection web site.

We concur with all four report recommendations that address collecting, monitoring, and evaluating Privacy Impact Assessments (PIAs) for all systems that collect personal identifiable information; establishing an electronic system to manage PIAs; monitoring IRS employee privacy awareness training; and reinforcing PIA case documentation and

implementing compliance reviews. Attached is a detailed response outlining our corrective action plans for each of the report recommendations. We appreciate your continued support and valuable oversight assistance. If you have any questions, please contact me at (202) 622-8910, or Barbra Symonds, Director, Office of Privacy and Information Protection at (202) 283-7373.

Attachment

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

RECOMMENDATION #1:

The Chief, Mission Assurance and Security Services, should request IRS business owners to identify and report all systems or projects that collect personal identifiable information. A Privacy Impact Assessment (PIA) should be prepared and submitted to the Office of Privacy and Information Protection for privacy evaluation, monitoring and oversight

CORRECTIVE ACTION TO RECOMMENDATION #1:

The following steps will be taken:

- The Office of Privacy and Information Protection will annually cross-walk PIA inventory to existing inventories, such as Federal Information Security Management Act and As-Built-Architecture, where information is being provided by the business owners, and identify systems that do not have a current PIA. The Business Owners are responsible to submit a PIA for evaluation to the Office of Privacy and Information Protection.
- The Office of Privacy and Information Protection will conduct a study to identify PIA process improvements to ensure that limited resources are focused on systems that collect or maintain personal identifiable information.
- The Office of Privacy and Information Protection will establish policy, based on the study, for systems and programs that require a PIA.

IMPLEMENTATION DATE:

October 15, 2007

RESPONSIBLE OFFICIAL:

Director, Office of Privacy and Information Protection, OS:MA:OPIP

CORRECTIVE ACTION MONITORING PLAN

The Office of Privacy and Information Protection maintains a comprehensive Work Breakdown Structure (WBS) that is updated on a weekly basis. The actions identified will be included in the WBS and progress reported on a Quarterly basis.

1

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

RECOMMENDATION #2:

The Director, Office of Privacy and Information Protection, should establish a centralized repository for all Privacy Impact Assessments (PIAs) in a searchable, electronic format. The process should be developed to verify the accuracy of the PIA inventory on a quarterly basis. The Office of Privacy and Information Protection should also develop an electronic document management system for archiving electronic PIA artifacts.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Several actions will be taken to address the recommendation.

a) The Office of Privacy and Information Protection is developing an electronic PIA inventory and will implement the inventory in FY2007.
b) The Office of Privacy and Information Protection will develop and implement a process to verify the PIA inventory accuracy on a quarterly basis. Sources for verification will be other system inventories, such as the Federal Information Security Management Act master inventory and As-Built-Architecture inventory.
c) The Office of Privacy and Information Protection is in the process of developing an electronic document management system for archiving electronic PIA artifacts. The Office will be moving PIA artifacts to a Sharepoint solution. Sharepoint will help maintain document management controls.

IMPLEMENTATION DATE:

a) October 15, 2007
b) October 15, 2007
c) February 15, 2008

RESPONSIBLE OFFICIAL:

a – c) Director, Office of Privacy and Information Protection, OS:MA:OPIP

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

CORRECTIVE ACTION MONITORING PLAN:

The Office of Privacy and Information Protection maintains a comprehensive Work Breakdown Structure (WBS) that is updated on a weekly basis. The actions identified will be included in the WBS and progress reported on a Quarterly basis.

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

RECOMMENDATION #3:

To monitor employee privacy awareness training, the Director, Office of Privacy and Information Protection, should initiate a program providing for the routine evaluation of employee training activities relative to current privacy policy requirements and develop a system for the tracking and monitoring of these activities.

CORRECTIVE ACTION TO RECOMMENDATION #3:

Several actions will be taken to address the recommendation.

a) The Office of Privacy and Information Protection is establishing privacy awareness training via the mandatory IRS Information Protection training. This training is mandatory for all employees. This training is to deploy via the IRS Enterprise Learning Management System (ELMS).
b) The Office of Privacy and Information Protection will develop and deploy an assessment methodology to survey IRS employees of their knowledge of the Office of Privacy and Information Protection and privacy policy requirements. The findings from the survey will provide the Office of Privacy and Information Protection with feedback on employee awareness and training needs. The assessment methodology will be deployed on an annual basis.
c) The Office of Privacy and Information Protection will initiate a job-specific training program for privacy. A job-specific, or role-based, training program is a Federal Information Security Management Act requirement. The Office of Privacy and Information Protection will conduct an assessment of roles that must be trained and will work to deploy role-based training via the ELMS.
d) In addition to role-based training, training modules on IRS privacy products, such as the Privacy Impact Assessment (PIA), will be developed for ELMS deployment in order to ensure accurate monitoring and tracking.

IMPLEMENTATION DATE:

a) October 15, 2007
b) October 15, 2008
c) October 15, 2008
d) October 15, 2007

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

RESPONSIBLE OFFICIAL:

a – d) Director, Office of Privacy and Information Protection, OS:MA:OPIP

CORRECTIVE ACTION MONITORING PLAN:

The Office of Privacy and Information Protection maintains a comprehensive Work Breakdown Structure (WBS) that is updated on a weekly basis. The actions identified will be included in the WBS and progress reported on a Quarterly basis.

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

RECOMMENDATION #4:

The Director, Office of Privacy and Information Protection, should reinforce the importance of Privacy Impact Assessments (PIAs) case documentation with specific instructions or case models and implement a compliance review process to assess whether IRS business units are adhering to privacy regulations, given limited resources and staff knowledge in conducting these reviews.

CORRECTIVE ACTION TO RECOMMENDATION #4:

Several actions will be taken to address the recommendation.

a) The Office of Privacy and Information Protection will establish assessment standards for PIAs to ensure consistency and extent of coverage based on system complexity. In addition, the Office will establish case documentation and analysis requirements, keeping in mind that analyst knowledge base will be part of the equation.
b) For the short-term, Office of Privacy and Information Protection will investigate tools, conduct a pilot of a selected tool, assess results, and implement interim measures to establish and implement compliance review guidelines and a process to ensure adherence to privacy regulations.
c) For the long-term, Office of Privacy and Information Protection will build on knowledge obtained in the second action above and implement comprehensive measures to establish and implement compliance review guidelines and a process to ensure adherence to privacy regulations. Since resources are limited, the task completion expectation is long-term.

IMPLEMENTATION DATE:

a) October 15, 2007
b) October 15, 2007
c) April 15, 2009

RESPONSIBLE OFFICIAL:

a – c) Director, Office of Privacy and Information Protection, OS:MA:OPIP

Management response to Draft Audit Report – The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements (Audit # 200620002)

CORRECTIVE ACTION MONITORING PLAN:

The Office of Privacy and Information Protection maintains a comprehensive Work Breakdown Structure (WBS) that is updated on a weekly basis. The actions identified will be included in the WBS and progress reported on a Quarterly basis.