TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses

July 24, 2006

Reference Number: 2006-20-111

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

Redaction Legend:

3d = Identifying Information - Other Identifying Information of an Individual or Individuals

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

July 24, 2006

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT
DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit # 200520034)

This report represents the results of our review to determine whether Internal Revenue Service (IRS) management and security staffs were adequately reviewing online Integrated Data Retrieval System (IDRS) reports to detect unauthorized accesses to taxpayer accounts.

Synopsis

The IDRS is a mission critical system containing sensitive information such as taxpayers' names, Social Security Numbers, birth dates, addresses, filing statuses, exemptions, and income. This System is used by IRS employees to research and update taxpayer data. Because of the sensitive nature of its data, the IDRS routinely generates audit trail[1] information. The IRS and Treasury Inspector General for Tax Administration use the audit trail information to identify unauthorized accesses to taxpayer accounts, thus ensuring employees who violate the Taxpayer Browsing Protection Act of 1997[2] are identified and appropriate employee actions are taken.

---

[1] An audit trail is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results.
[2] 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003). This Act makes it a criminal offense to access or inspect tax information without proper authorization. This legislation focuses on the IRS ensuring its employees access taxpayer data only for official purposes.

Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses

In 2002, the IRS incrementally deployed the IDRS Online Reports Services (IORS) system[3] to reduce the costs of printing and distributing paper reports of IDRS audit trail information to IRS personnel responsible for identifying unauthorized accesses. However, audit trail information from the IORS system was not always being reviewed and investigated to detect unauthorized accesses and noncompliance with security controls.

A majority of IRS managers are not reviewing IDRS Security Reports. As a result, IRS employees may be browsing their spouses' or other employees' tax accounts with little chance of detection.

Although 9 of the 10 campus[4] data security staffs carried out their security-related responsibilities for reviewing IDRS Security Reports using the IORS system, a majority of business unit managers are not performing their responsibilities to investigate potential unauthorized accesses to IDRS accounts and noncompliance with security controls. As a result, employees may be browsing their spouses' or other employees' tax information with little chance of detection. In addition, employees may be knowingly or unknowingly violating current security procedures that could enable unauthorized persons to access sensitive taxpayer information. For instance, during one of our site visits, we identified [3(d)]

[5]

Using the IORS system, IRS business unit managers are responsible for reviewing and certifying four IDRS Security Reports. On average, only 42 percent of IRS business unit managers certified their IDRS Security Reports in September 2005. Individual campus certification rates[6] ranged from a high of 75 percent to a low of 15 percent, and only 36 percent of these certifications were performed timely. The Mission Assurance and Security Services (MA&SS) organization and IRS business unit management have not sufficiently emphasized the need for business unit managers to review the IDRS Security Reports produced by the IORS system. In addition, managers were not held accountable for reviewing the IDRS Security Reports on a regular basis, and the level of emphasis varied among the data security staffs located at the IRS campuses.

---

[3] The IORS system is a web-based application that provides business unit managers and data security staffs online access to security reports based on the IDRS audit trail information.

[4] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

[5] The IRS conducts awareness briefings to better focus agency-wide attention on preventing the willful unauthorized access and inspection of taxpayer records, which it refers to as UNAX.

[6] Campus certification rates are based on certification rates of all Area Offices serviced by a particular campus. Area Offices are located throughout the United States; they serve as the coordination point for and assist the public with tax issues.

Due to the low certification rates nationally, we have little confidence that IRS managers are detecting potential unauthorized accesses of taxpayer information by employees. Additionally, the IRS cannot ensure employees are complying with the security controls established to protect the IDRS.

During our visits to the IRS Campuses in Brookhaven, New York, and Austin, Texas, we found the compliance levels were directly affected by the amount of emphasis provided by the local data security staffs. For example, the data security staff at the Brookhaven Campus made the effort to communicate with employees at the Campus and in the Area Offices, provide local IORS system users with training and awareness information, and notify senior business unit managers when subordinate managers did not review IDRS Security Reports timely. As a result, the certification rate was 75 percent. Conversely, the Austin Campus was not providing adequate emphasis over the IORS system program, and its compliance rate was only 15 percent.

Systemic problems with the IORS system also contributed to the low levels of compliance. These problems hindered business unit managers from adequately reviewing and timely identifying potential unauthorized accesses to employees' and their spouses' accounts and noncompliance with security controls on the IDRS. For example, certain IORS system users were unable to retrieve IDRS Security Reports, and slow response times hindered business unit managers' reviews of IDRS Security Reports.

The IRS paid a contractor $2.4 million over 3 years to develop the IORS system and took incremental delivery of it in 2002, although the IORS system did not completely meet the IRS' requirements. Additional system enhancements to address deficiencies were to be made in the next version of the IORS system, originally scheduled for deployment in December 2005. However, the MA&SS organization determined the contractor was unable to develop the new version of the IORS system according to the IRS' needs, and the contract, which expired in September 2005, was not renewed.

Recommendations

We recommended the Chief, MA&SS, (1) emphasize to the IRS business units the need to review electronic IDRS Security Reports using the IORS system and (2) eliminate the requirement to certify the monthly Security Profile Report[7] to reduce managerial burden. Additionally, we recommended the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement ensure business unit managers' operational review requirements are updated to include a step to validate the certification of IDRS Security Reports. Business unit managers should then be held accountable for meeting their security-related responsibilities.

[7] The Security Profile Report is a monthly and quarterly IDRS security report that identifies employees' capabilities on the IDRS and occurrences when employees use a command that is not within their user profiles.

To complete development of the next version of the IORS system, we recommended the Chief, MA&SS, place priority on hiring a new contractor and prioritize and address the systemic weaknesses within a reasonable time period.

Response

The IRS agreed with three of the four recommendations in our report and disagreed with one. To ensure IDRS Security Reports are reviewed in the future, the IRS will implement a process to monitor and review the compliance rate of IRS business units. Actions will be taken to require all IRS business units to include the results of MA&SS organization quarterly compliance reports in all management operational reviews to identify and enforce consequences for noncompliance. The IRS will address all the systemic weaknesses connected with the IORS system and will obtain contractual support to ensure all weaknesses are corrected. The IRS disagreed with our recommendation that certification of the monthly Security Profile Report be eliminated, due to the length of time between the quarterly and monthly reporting periods. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment

In our discussion draft report, we initially recommended the IRS eliminate the quarterly Security Profile Report because the IRS already had a requirement to certify the monthly versions of this Report. During the closing conference on the discussion draft report, MA&SS organization representatives requested that we instead recommend eliminating the monthly Security Profile Report, to reduce the burden to IRS managers. We concurred with the request and revised our recommendation accordingly. Management's disagreement with this recommendation is contradictory to what was discussed at our closing conference. We continue to believe the IRS should take whatever actions are needed to ensure the security and privacy of taxpayer data on the IDRS.

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

Audit Trail Information Is Not Always Being Reviewed and Investigated to Identify Unauthorized Accesses to Taxpayer Accounts ..... Page 3

Recommendations 1 and 2: ..... Page 8

Recommendation 3: ..... Page 9

Systemic Problems Are Hindering Management Reviews for Unauthorized Accesses to Taxpayer Accounts ..... Page 9

Recommendation 4: ..... Page 11

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 12

Appendix II – Major Contributors to This Report ..... Page 14

Appendix III – Report Distribution List ..... Page 15

Appendix IV – Management's Response to the Draft Report ..... Page 16

Abbreviations

IDRS	Integrated Data Retrieval System
IORS	IDRS Online Reports Services
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access to Taxpayer Information

Background

The Taxpayer Browsing Protection Act of 1997[1] made it a criminal offense to access or inspect tax information without proper authorization. A person convicted of any such violation shall be dismissed and be subject to a fine of up to $1,000, imprisonment of not more than 1 year, or both. This legislation was essentially focused on the Internal Revenue Service (IRS) to ensure its employees access taxpayer data only for official purposes. One of the main systems used by IRS employees to research and update taxpayer data is the Integrated Data Retrieval System (IDRS). The IDRS is a mission critical system that contains sensitive information such as taxpayers' names, Social Security Numbers, birth dates, addresses, filing statuses, exemptions, and income.

Because of the sensitive nature of its data, the IDRS routinely generates audit trail[2] information that can be used to detect potential unauthorized accesses to taxpayer accounts. The IRS refers to the unauthorized access of taxpayer information as UNAX and provides yearly training to all employees to protect against it. Data security staffs located in the 10 IRS campuses[3] and business unit managers located throughout IRS offices must investigate accesses to employees' and their spouses' accounts to determine whether the accesses were made for business reasons. In addition, business unit managers should review audit trail information to detect noncompliance with security controls. For example, multiple failed attempts to access an account could indicate an unauthorized person was attempting to guess a password to gain access to sensitive data. Business unit managers should also review audit trail information to ensure employees have access to only the computer command codes[4] they need to carry out their business responsibilities.

The IDRS Online Reports Services system is a web-based application that provides business unit managers and data security staffs online access to IDRS Security Reports based on the IDRS audit trail information.

For many years, IRS data security staffs and business unit managers received IDRS audit trail information in computer-generated paper reports. To reduce the costs of printing and distributing these reports and to improve the effectiveness of reporting results of

[1] 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).
[2] An audit trail is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results.
[3] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[4] These are various IDRS entry codes employees can use to research tax account information and update tax accounts.

management reviews, the IRS deployed the IDRS Online Reports Services (IORS) system in 2003. The IORS system gives business unit managers the ability to retrieve, review, and comment on IDRS Security Reports electronically. The IORS system report content is used to identify authorized IDRS users who are attempting to perform unauthorized accesses, unauthorized attempts to access the IDRS, and users who need additional training because of repeated errors that could compromise the security of the System. Business unit managers can also use the IORS system to request archived IDRS Security Reports for data analyses and to initiate and approve IDRS security forms.

The Mission Assurance and Support Services (MA&SS) organization is responsible for overseeing compliance with the IORS system and has direct responsibility over data security staffs located in the IRS campuses. Business units are responsible for ensuring their managers comply with IORS system procedures by investigating potential security violations and taking appropriate corrective actions. The data security staffs in each campus also monitor business unit managers in the campuses and the offices supported by those campuses to ensure IDRS Security Reports produced by the IORS system are properly reviewed. For example, the IRS Campus in Brookhaven, New York, is responsible for monitoring the Boston Area Office.[5]

In addition to IRS monitoring of the IDRS, the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations Strategic Enforcement Division conducts comprehensive proactive reviews of IDRS audit trail information to identify other unauthorized accesses, such as unauthorized accesses of tax information of celebrities, political figures, and employees' neighbors, former spouses, and relatives. Over the past 2 fiscal years, the TIGTA initiated 990 UNAX cases. All of the reviews of IDRS audit trail information performed by the IRS and the TIGTA should provide assurance that employees who violate the Taxpayer Browsing Protection Act of 1997 are identified and appropriate employee actions are taken.

This review was performed at the Brookhaven and Austin, Texas, Campuses; the Boston, Massachusetts, and Houston, Texas, Area Offices; and the MA&SS organization office in New Carrollton, Maryland, during the period June 2005 through February 2006. These locations were selected based on the campuses with the highest and lowest IDRS Security Report certification rates. 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.

[5] Area Offices are located throughout the United States; they serve as the coordination point for and assist the public with tax issues.

Results of Review

Audit Trail Information Is Not Always Being Reviewed and Investigated to Identify Unauthorized Accesses to Taxpayer Accounts

The data security staffs in 9 of the 10 campuses carried out their security-related responsibilities for reviewing IDRS Security Reports produced by the IORS system. However, a majority of business unit managers are not performing their responsibilities to investigate potential unauthorized accesses to IDRS accounts and noncompliance with security controls. As a result, employees may be browsing their spouses' or other employees' tax accounts with little chance of detection. During 1 of our site visits, we found β(d) a clear violation of the UNAX program. In addition, employees may be knowingly or unknowingly violating current security procedures that could enable unauthorized persons to access sensitive information.

A majority of IRS managers are not reviewing IDRS Security Reports. As a result, IRS employees may be browsing their spouses' or other employees' tax accounts with little chance of detection.

Business unit managers are not always reviewing IDRS Security Reports on the IORS system

IRS business unit managers are responsible for reviewing and certifying the following four IDRS Security Reports using the IORS system.

- ***Sensitive Access Report*** – Issued weekly; identifies IRS employees who have accessed another employee's or an employee's spouse's tax accounts. The IRS requires business unit managers to determine whether employees made these accesses for work-related reasons. Business unit managers must take appropriate steps, including research on the IDRS and review of case assignment files, to identify the employees' reasons for the accesses. If needed, business unit managers may also interview the employees.
- ***Security Violations Report*** – Issued weekly; identifies unsuccessful logon attempts and employees who left their computers without logging off. Business unit managers should discuss these violations with their employees to determine whether unauthorized persons were trying to guess their passwords and whether the employees need additional training on using the IDRS.
- ***IDRS Security Profile Reports (2 reports)*** – Issued monthly and quarterly; identify employees' capabilities on the IDRS and attempted accesses to taxpayer accounts using

unauthorized command codes. Business unit managers should review these Reports to ensure employees only have the access capabilities they need to perform their responsibilities and to determine whether all attempted accesses to taxpayer accounts using unauthorized command codes were unintentional errors.

The IRS requires business unit managers to review and certify the weekly IDRS Security Reports within 14 calendar days of receipt and the monthly and quarterly Security Profile Reports within 28 calendar days of receipt. The IORS system determines whether business unit managers are responding timely to the Security Reports and sends email notifications to managers who have not responded within the specified period.

For September 2005, only 42 percent of IRS business unit managers certified their IDRS Security Reports. Individual campus certification rates for September 2005 ranged from a high of 75 percent to a low of 15 percent. Only 36 percent of these certifications were performed timely. Figure 1 presents the compliance levels for each of the 10 IRS campuses. The results for each campus include the certification and timeliness rates for all IRS offices supported by the data security staffs in the campuses.

Figure 1: National IORS System Compliance Levels

IRS Campus	Certification Rate	Timeliness Rate
1. Andover	53%	47%
2. Atlanta	33%	28%
3. Austin	15%	13%
4. Brookhaven	75%	69%
5. Cincinnati	34%	29%
6. Fresno	35%	29%
7. Kansas City	50%	40%
8. Memphis	24%	19%
9. Ogden	66%	57%
10. Philadelphia	34%	31%
Averages	**42%**	**36%**

Source: September 2005 compliance levels based on the MA&SS organization's analyses.[6]

[6] The national IORS system compliance levels were computed manually by the MA&SS organization. Additionally, IDRS Security Reports issued to managers for certification with no violations reported were not used in the analysis.

The certification rates and timeliness rates were consistently low for the four IDRS Security Reports that business unit managers are required to review. Figure 2 reflects the September 2005 compliance levels for the four Reports.

Figure 2: IORS System Compliance Levels by Report

Security Report Type	Certification Rate	Timeliness Rate
1. Weekly Sensitive Access	46%	34%
2. Weekly Security Violations	50%	39%
3. Monthly Security Profile	40%	40%
4. Quarterly Security Profile	32%	32%
Averages	**42%**	**36%**

Source: September 2005 compliance levels based on the MA&SS organization's analyses.

Two of the Reports (the monthly and quarterly IDRS Security Profile Reports) provide the same information but cover different time periods. Reviews of the quarterly Security Profile Reports were the lowest among all four IDRS Security Reports. IRS business unit managers advised us that either the certification of the monthly or the quarterly Security Profile Report could be eliminated, or the Report results could be provided for informational purposes only.

The MA&SS organization and IRS business units have not sufficiently emphasized the need for business unit managers to review IDRS Security Reports and have not held their managers accountable for reviewing these Reports on a regular basis. Due to the low certification rates nationally, we have little confidence that IRS managers are detecting all potential unauthorized accesses of taxpayer information. Additionally, without these reviews, the IRS cannot ensure employees are complying with the security controls established to protect the IDRS.

We noted a wide disparity in the amount of emphasis provided by the data security staffs in the campuses. Specifically, we found the compliance levels for the Brookhaven and Austin Campuses were directly affected by the amount of emphasis provided by the local data security staffs. The data security staff in the Brookhaven Campus effectively communicated with employees at the Campus and in the Area Offices and notified senior business unit managers when subordinate managers did not review IDRS Security Reports timely. This information was shared with the manager responsible for certifying the Reports.

The Brookhaven Campus data security staff also supported IORS system users through the use of several IORS system instructional materials, training lessons, and newsletters. Instructional aids were prepared to assist business unit managers in the review and certification of IDRS Security Reports. Limited IORS system training was developed locally and provided to employees on an

as-requested basis. In addition, quarterly newsletters were issued to inform business unit managers of important IORS system features and problems that hinder the review of IDRS Security Reports. As a result, most Brookhaven Campus business unit managers regularly reviewed IDRS Security Reports.

Conversely, the Austin Campus was not providing adequate emphasis over the IORS system program to ensure employees were reviewing IDRS Security Reports. The [redacted] business unit managers we interviewed in the Houston Area Office had not reviewed any of the required 579 IDRS Security Reports in Fiscal Year 2005. The business unit managers indicated a significant lack of emphasis and support on how to initially access the IORS system by the Austin Campus data security staff. 3(d)

Additionally, 104 (28 percent) of the 370 business unit managers at the Austin Campus had never logged into the IORS system, although training was provided in 2003. Because these business unit managers failed to log in, IORS system user accounts were not established.

As a result, business unit managers were not receiving IDRS Security Reports showing potential inappropriate transactions and noncompliance with security controls for over 1,400 Austin Campus employees. Because these IRS managers did not initially log into the IORS system, IDRS Security Reports were not provided for these managers and could not be reviewed to detect inappropriate activity. Figure 3 provides a breakout by function of the business unit managers assigned to the Austin Campus who have never logged into the IORS system.

Figure 3: IRS Functional Managers Not Using the IORS System - Austin Campus

IRS Function	Number of Managers	Number of Employees
1. Submission Processing	3(d)	3(d)
2. Accounts Management		
3. Compliance		
4. Criminal Investigation Fraud		
5. Austin Information Systems		
6. Austin IORS Specific Users		
7. Wage and Investment		
8. Appeals		
Total	**104**	**1,429**

Source: The MA&SS organization's analyses, September 2005.

Most data security staffs certify they reviewed IDRS Security Reports

On a daily basis, data security staffs located in each IRS campus are required to certify they have reviewed the four IDRS Security Reports generated daily. Specifically, the Sensitive Access Report identifies IDRS users with attempted and actual accesses to another employee's or an employee's spouse's tax accounts. The three other Reports are designed to ensure the accuracy of the IORS system and monitor overall usage by command codes.

For Fiscal Year 2005, data security staffs in each of the 10 IRS campuses certified 94 percent of the IDRS Security Reports. Eighty-seven percent of these Reports were timely certified (within 7 calendar days of the managers' receipt of the Report). The Sensitive Access Report certification rates ranged nationally from a high of 100 percent at the Andover, Atlanta, and Kansas City Campuses to a low of 51 percent at the Memphis Campus. Figure 4 presents the Fiscal Year 2005 Sensitive Access Reports compliance levels for each of the 10 IRS campus data security staffs.

Figure 4: National Sensitive Access Reports Compliance Levels for Fiscal Year 2005 - Data Security Staffs

IRS Campus	Certification Rate	Timeliness Rate
1. Andover	100%	99%
2. Atlanta	100%	99%
3. Austin	94%	91%
4. Brookhaven	94%	88%
5. Cincinnati	95%	65%
6. Fresno	89%	86%
7. Kansas City	100%	76%
8. Memphis	51%	42%
9. Ogden	97%	86%
10. Philadelphia	97%	89%
Averages	**94%**	**87%**

Source: The MA&SS organization's analyses.

The Memphis Campus certified only 24 (51 percent) of the 47 Sensitive Access Reports in Fiscal Year 2005, and only 42 percent of the reports were timely reviewed. These Reports are crucial for identifying users who attempted to access tax records of another employee or an employee's spouse's account. These accesses are prohibited under the Taxpayer Browsing Protection Act of 1997 and could indicate employees who are attempting to improperly alter

their own or their spouses' tax accounts. Although the IDRS should block such accesses, the data security staffs are required to report the employees to the IRS Labor Relations Office[7] for control and assignment to the employees' managers for an official response. In some instances, if the access was inappropriate, the case should be referred to the TIGTA Office of Investigations. We attribute the noncompliance at the Memphis Campus to a lack of local emphasis and oversight by the MA&SS organization.

Recommendations

Recommendation 1: The Chief, MA&SS, should coordinate with the business units and place emphasis on the review of electronic IDRS Security Reports using the IORS system. Periodic compliance reviews should be conducted to ensure the business units carry out their roles and responsibilities to review IDRS Security Reports.

> ***Management's Response:*** The IRS agreed with this recommendation. The MA&SS organization will implement a semiannual monitoring and reporting process that will determine compliance of the IRS business units with requirements to review and certify IDRS Security Reports. IRS business units will be advised of their compliance.

Recommendation 2: The Chief, MA&SS, should eliminate the requirement to certify the monthly Security Profile Report to reduce managerial burden because the data are captured in the quarterly Security Profile Reports.

> ***Management's Response:*** The IRS disagreed with this recommendation, stating that deferring the review of the Security Profile Report to only quarterly periods could result in various deficiencies going undetected for extended periods.
>
> ***Office of Audit Comment:*** In our discussion draft report, we initially recommended the IRS eliminate the quarterly Security Profile Report because the IRS already had a requirement to certify the monthly versions of this Report. During the closing conference on the discussion draft report, MA&SS organization representatives requested that we instead recommend eliminating the monthly Security Profile Report, to reduce the burden to IRS managers. We concurred with the request and revised our recommendation accordingly. Management's disagreement with this recommendation is contradictory to what was discussed at our closing conference. We continue to believe the IRS should take whatever actions are needed to ensure the security and privacy of taxpayer data on the IDRS.

[7] This is the IRS office that reviews proposed employee disciplinary actions and ensures actions are consistent and in conformance with laws, rules, regulations, and prior judicial and appeal decisions.

Recommendation 3: The Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement should ensure all business unit managers' operational review requirements are updated to include a step to validate that all IORS system-related reports are certified timely (by the manager or designee) and to hold the business unit managers accountable for meeting their security-related responsibilities.

> ***Management's Response:*** The IRS agreed with this recommendation. A memorandum will be issued by the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement to all IRS Commissioners and Chiefs requiring all business units' operational reviews to include MA&SS organization quarterly IORS security compliance reports and to identify and enforce consequences for noncompliance.

Systemic Problems Are Hindering Management Reviews for Unauthorized Accesses to Taxpayer Accounts

In addition to a lack of emphasis, we attribute some of the noncompliance by business unit managers to systemic problems. These problems involve significant system access and software issues, which have hindered managers' ability to review IDRS Security Reports timely using the IORS system. The IORS system should effectively facilitate the distribution, review, and accurate validation of IDRS reports, and, when necessary, responsive action to the contents of these reports.

Systemic problems with the IORS system hinder business unit managers from adequately reviewing and timely identifying potential unauthorized IDRS accesses.

The IRS paid a contractor $2.4 million over 3 years to develop the IORS system. The IRS took delivery of the IORS system incrementally starting in 2002 and during 2003 relied on it to assist with the identification of unauthorized accesses and noncompliance with security controls. Although the IORS system is operational, the following systemic issues and problems are hindering business unit managers from adequately reviewing and timely identifying potential unauthorized accesses to employees' and their spouses' accounts and noncompliance with security controls on the IDRS.

System access issues

Slow response times have hindered business unit managers' reviews of IDRS Security Reports. Several business unit managers we interviewed stated they had experienced significant amounts of system downtime and slow IORS system performance. Business unit managers also discussed the difficulty reviewing IDRS Security Reports on Mondays due to the large number of users attempting to log into the IORS system. The IORS system application was moved to a single server in August 2005 and users saw some improvement. An even more dramatic improvement in performance was achieved when the MA&SS organization implemented

automated maintenance routines in October 2005. The MA&SS organization stated that, in the future, it will be providing its employees with database and web-server administration training regarding procedures to optimize performance of the IORS system servers.

Certain IORS system users are unable to retrieve IDRS Security Reports. When they attempt to retrieve the IDRS Security Reports, the IORS system logs them out and then displays the IORS system login page. The problem occurs if the users connect to the IORS system web site using a "shortcut" or "favorites" link they created while logged into the IORS system. Users are instructed to go to the IORS system web site and log in when they experience this situation.

Some business unit managers are unable to access the monthly and quarterly IDRS Security Profile Reports. On occasion, users receive an error message when they attempt to retrieve these Reports. As an alternative, the MA&SS organization developed a program to run every 3 minutes to recompile the IORS system database table that supports these Reports.

The IORS system issues "certification due" notices even when managers have no IDRS Security Reports to review. The MA&SS organization suggested that users certify the blank Reports to prevent an erroneous reminder notice. The Reports could be suppressed to minimize management burden.

Software problems

A software problem in the IORS system application causes IDRS Security Reports to display only the certifications that were input by the current manager. The certification information will not appear if a Security Report was certified by someone else.

The IORS system feature to track certification and timeliness rates provides inaccurate results when managers designate another manager to certify an IDRS Security Report. Business unit managers in the Brookhaven Campus instead keep track manually using a locally developed checklist of Security Reports they have certified.

A software problem allows IORS system user profiles and permissions to be transferred to other business unit managers. Business unit managers are then able to view and certify other business unit managers' and employees' security reports.

Management oversight issues

Business unit managers have the ability to review and certify their own security violations without requiring a higher level of approval. Business unit managers' violations are displayed on the same IDRS Security Report as those of their employees. According to the Brookhaven Campus data security staff, the issue was discussed with the MA&SS organization and an oversight feature was developed in the IORS system to address the problem. The feature allows program managers to log into the IORS system to review violations committed by their business unit managers. However, the use of this feature is voluntary, and only one program manager at the Brookhaven Campus was using it. When business unit managers are allowed to approve

their own violations, the IRS is offering managers unlimited access to taxpayer account data and allowing unauthorized accesses to go undetected.

Most business unit managers are not using the IORS system proxy feature. The Brookhaven Campus data security staff discouraged its use because of system problems. The proxy feature should be used to assign another user to review reports when business unit managers are not available. Our interviews of 50 managers indicated users are not fully aware of the importance of this feature. For example, 1 manager 3(d) and did not assign a proxy to review the security reports for 3(d) employees during the absence.

During our review, the MA&SS organization began development of a web site to track the ongoing systemic issues with the IORS system. Business unit managers will be able to access the web site to obtain current information on problems with the application and on alternatives to use until the deficiencies are fixed. This web site became operational in April 2006.

The IRS was aware the IORS system did not completely meet its requirements when it took incremental delivery in 2002. Additional enhancements to address deficiencies were to be included in the next version of the IORS system, originally scheduled for deployment in December 2005. However, the MA&SS organization determined the contractor was unable to develop the new version of the IORS system according to the IRS' needs. The contract, which expired in September 2005, was not renewed, and deployment of the new version has been delayed.

Recommendation

Recommendation 4: The Chief, MA&SS, should place priority on hiring a new contractor to complete development of the next version of the IORS system. The systemic weaknesses with the IORS system should be prioritized and addressed within a reasonable time period.

> ***Management's Response:*** The IRS agreed with this recommendation. The MA&SS organization is coordinating with the Chief Information Officer to transfer the responsibility of obtaining the technical contract for the IORS system. The MA&SS organization IDRS Security Program Office will prioritize the systemic weaknesses of the IORS system and monitor the process for timely implementation of systemic changes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether IRS management and security staffs were adequately reviewing online IDRS[1] reports to detect unauthorized accesses to taxpayer accounts. To accomplish our objective, we:

I. Determined whether managers of IDRS users, designated proxies,[2] and unit security representatives[3] were carrying out their responsibilities for identifying potential unauthorized access violations by evaluating national IORS system[4] reports for all 10 IRS campuses.[5]

A. Evaluated the guidance, oversight, and training provided by the MA&SS organization to the field offices responsible for conducting security reviews to ensure adherence to applicable guidelines and criteria.

B. Determined whether sufficient training on the IORS system had been timely provided to managers, designated proxies, and data security staffs.

C. Determine whether data security staffs and business unit managers were complying with the requirements to review IDRS Security Reports to detect unauthorized accesses to taxpayer accounts. We reviewed national statistics for all 10 IRS campuses and visited the Brookhaven, New York, and Austin, Texas, Campuses. We also visited the Boston, Massachusetts, and Houston, Texas, Area Offices[6] and reviewed the IORS reports for Fiscal Year 2005 for 50 managers we

[1] The IDRS is the IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[2] The designated proxies review the security reports when the business unit managers are not available.
[3] Unit security representatives are individuals assigned by their business organizations to help ensure IDRS security administration activities are properly performed for their IDRS users.
[4] The IORS system is a web-based application that provides business unit managers and data security staffs online access to IDRS Security Reports based on the IDRS audit trail information. An audit trail is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results.
[5] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[6] Area Offices are located throughout the United States; they serve as the coordination point for and assist the public with tax issues.

judgmentally selected.[7] We could not identify the population of managers due to systemic errors with the IORS system. The Area Offices were selected based on the Brookhaven and Austin Campuses, which had the highest and lowest IDRS Security Report certification rates, respectively.

D. Contacted the Treasury Inspector General for Tax Administration Office of Investigations local offices before our visits to determine whether they had any ongoing investigations in the sampled offices.

II. Determined whether the IORS system web-based application was operating effectively and met the needs of its users.

A. Interviewed the program analyst and developers in the MA&SS organization to determine whether the IORS system application was working as intended.

B. Determined the future plans for or enhancements to be made to the IORS system.

C. Evaluated the weekly, monthly, and quarterly IDRS Security Reports to determine whether the information was presented in a clear and understandable format.

D. Visited the Campuses and Area Offices with the highest and lowest IORS report certifications rates. The sites included the Brookhaven and Austin Campuses and the Boston and Houston Area Offices.

E. Selected a judgmental sample of 50 business unit managers at the 4 locations visited. We could not identify the population of managers due to systemic errors with the IORS system. We interviewed the managers and the data security staffs at the Brookhaven and Austin Campuses to determine whether the IORS system operated effectively and met the needs of its users.

[7] We used judgmental sampling for Steps I.C. and II.E. due to time constraints and availability of managers during our site visits.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Acting Director
Thomas Polsfoot, Audit Manager
Michelle Griffin, Senior Auditor
Abraham Millado, Senior Auditor
Jacqueline Nguyen, Senior Auditor
William Simmons, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Chief Information Officer OS:CIO
Chief, Mission Assurance and Security Services OS:MA
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 Liaisons:
- Deputy Commissioner for Operations Support OS
- Deputy Commissioner for Services and Enforcement SE
- 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

RECEIVED
JUL 06 2006

CHIEF
MISSION ASSURANCE

JUL 06 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: for Daniel Galik
Chief, Mission Assurance and Security Services

SUBJECT: Response to Draft Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Access (Audit # 200520034)

Thank you for the opportunity to review the draft audit report on IRS' Integrated Data Retrieval System Online Reports Services (IORS), a web-based application that provides Integrated Data Retrieval System (IDRS) security reports to Unit Security Representatives and managers. The IDRS is a main system used by IRS employees to research and update taxpayer data. We appreciate that your report credits the IRS for deploying IORS to reduce the costs of printing and distributing paper copies of computer-generated IDRS audit trail report information.

The report has four recommendations. We concur on three of the report recommendations and non-concur on the remaining one recommendation. Attached is a detailed response outlining our corrective action plans to the recommendations. Specifically, for recommendation #1, you addressed IRS emphasizing the review of IORS reports. Actions will be taken to implement a process to monitor review compliance by Business Units. In recommendation #2, you propose eliminating the certification of the monthly Security Profile Report. We do not concur, the IRS is concerned that deferring the review of Security Profile Report to only quarterly periods could result in a potential security deficiency being undetected for an extended period of time. Recommendation #3 addresses timely certification of the reviews of IORS reports and management accountability. Actions will be taken requiring the timely reviews and addressing noncompliance. The final recommendation addresses contractual support of IORS. This is a priority of the Service to ensure system weaknesses are corrected.

We appreciate your continued support and valuable oversight assistance. If you have any questions, please contact me at (202) 622-8910, or Devon Bryan, Director, Information Technology Security at (202) 283-7271.

Attachment

Management response to Draft Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit #200520034)

RECOMMENDATION #1:
The Chief, Mission Assurance and Security Services, should coordinate with the business units and place emphasis on the review of electronic IDRS Security Reports using the IORS system. Periodic compliance reviews should be conducted to ensure the business units carry out their roles and responsibilities to review IDRS Security Reports.

CORRECTIVE ACTION TO RECOMMENDATION #1:
Mission Assurance and Security Services concurs with the recommendation and will implement a semiannual monitoring and reporting process that will determine compliance of the business units in reviewing and certifying Integrated Data Retrieval System (IDRS) Security reports. Business units will be advised of their compliance.

IMPLEMENTATION DATE:
December 15, 2006 (First compliance check is for the third and forth quarters of FY 2006)

RESPONSIBLE OFFICIAL:
Director, Information Technology Security OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:
The IDRS Security Program Office will report monthly to the Director, IT Security, on the progress of developing the applications and procedures to implement a monitoring and reporting process. Also, once implemented, all business units that do not achieve at least a 90 percent certification rate will be required to provide a justification for the report not being reviewed.

Management response to Draft Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit #200520034)

RECOMMENDATION #2:
The Chief, Mission Assurance and Security Services, should eliminate the requirement to certify the monthly Security Profile Report to reduce managerial burden because the data is captured in the quarterly Security Profile Reports.

CORRECTIVE ACTION TO RECOMMENDATION #2:
Mission Assurance and Security Services does not concur with this recommendation. The Integrated Data Retrieval System (IDRS) Security Profile reports summarize user activities and capabilities on IDRS on both a monthly and quarterly basis. Deferring the review of this report to only quarterly periods could result in various deficiencies being undetected for extended periods of time. Such deficiencies would include identifying IDRS users who are in the wrong units, who need a restriction applied to their profile in accordance with IRS policies, or who no longer need access to IDRS. By requiring the review and certification of the quarterly report, managers can better determine whether users have command codes and accesses to other IDRS functionality that are no longer needed.

IMPLEMENTATION DATE:
Not Applicable

RESPONSIBLE OFFICIAL:
Not Applicable

CORRECTIVE ACTION MONITORING PLAN:
Not Applicable

Management response to Draft Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit #200620034)

RECOMMENDATION #3:
The Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement should ensure all business unit managers' operational review requirements are updated to include a step to validate that all IORS system-related reports are certified timely (by the manager or designee) and to hold the business unit managers accountable for meeting their security-related responsibilities.

CORRECTIVE ACTION TO RECOMMENDATION #3:
The IRS concurs with the recommendation. A memo signed jointly by the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement will be issued to IRS Commissioners and Chiefs:

(1) Requiring all Business Units' operational reviews to include Mission Assurance and Security Services IORS quarterly Integrated Data Retrieval System (IDRS) security compliance reports.
(2) Identifying and enforcing consequences for noncompliance in reviewing and certifying the IDRS security compliance reports maintained in IORS.

IMPLEMENTATION DATE:
December 15, 2006

RESPONSIBLE OFFICIAL:
Deputy Chief, Mission Assurance & Security Services OS:MA

CORRECTIVE ACTION MONITORING PLAN:
Mission Assurance and Security Services will be tracking the development of the memo until distribution.

Management response to Draft Audit Report – Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit #200520034)

RECOMMENDATION #4:
The Chief, Mission Assurance and Security Services, should place priority on hiring a new contractor to complete development of the next version of the IORS system. The systemic weaknesses with the IORS system should be prioritized and addressed within a reasonable time period.

CORRECTIVE ACTION TO RECOMMENDATION #4:
Mission Assurance and Security Services (MA&SS) concurs with this recommendation. MA&SS has placed a priority on obtaining technical support. MA&SS is coordinating and working with the Chief Information Officer's organization to transfer the responsibility of obtaining the technical contract for the IORS system. The CIO organization will use existing contracting vehicles to fulfill the needed contractual support. Also, MA&SS' IDRS Security Program Office will prioritize the systemic weaknesses of IORS and monitor the process for timely implementation of system changes.

IMPLEMENTATION DATE:
November 15, 2006

RESPONSIBLE OFFICIAL:
Director, Information Technology Security OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:
The Director for the IT Security Office will periodically monitor the progress in obtaining contractual support and correcting IORS programming deficiencies.