Progress Has Been Made, but Additional Steps Are Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses

September 9, 2009

Reference Number: 2009-20-119

Redaction Legend:

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 9, 2009

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER
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 – Progress Has Been Made, but Additional Steps Are Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses (Audit # 200820020)

This report presents the results of our review to evaluate compliance by Internal Revenue Service (IRS) management and security staffs in reviewing and certifying Integrated Data Retrieval System (IDRS)[1] security reports, which are produced online by the IDRS Online Report Services (IORS) system, and assess whether corrective actions taken to address our prior audit findings[2] were effective. This audit was part of the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of our statutory requirement to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

The IRS requires managers of IDRS users to review and respond to IDRS security reports on the IORS system that present questionable accesses to the taxpayer accounts. While the national averages of certification and timeliness rates have improved, the IRS did not ensure that all IDRS business divisions were completing their responsibilities for reviewing and certifying IDRS security reports. Until additional improvements are made, the IRS cannot ensure that taxpayer

[1] IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[2] *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 24, 2006).

accounts on its primary tax account system are being properly protected from unauthorized accesses.

Synopsis

About 50,000 IRS employees access the IDRS to process taxpayer data during the course of their normal work duties. Managers of IDRS users are required to review and certify IDRS security reports on the IORS system on a regular basis to ensure that employee accesses to the IDRS are for valid work reasons. The IRS requires that managers maintain at least a 90 percent certification rate.

During Fiscal Year 2005, only 54 percent of IDRS security reports were certified. During this review, we found that 89 percent of IDRS security reports were certified for Fiscal Year 2008. We attribute this significant improvement to the Cybersecurity organization IDRS Security Program staff's actions to improve and enhance the IORS system. The IDRS Security Program staff corrected prior system problems that were hindering IDRS managers' ability to access IDRS security reports. For example, they implemented new systemic features, such as automatic email messages to remind IDRS managers when certifications are due, a "report certification due" box on IORS system report screens that displays any reports that have not been certified and highlights past due reports in red, and weekly reports for distribution by IDRS security officers that list which IDRS managers have and have not completed certifications.

While the national averages of certification and timeliness rates have improved, more needs to be done to ensure that all taxpayer accounts are protected from unauthorized access. Of the total 325,475 security reports requiring certification by IDRS managers in Fiscal Year 2008, 36,493 (11 percent) were not reviewed and certified, potentially allowing improper accesses to go undetected. The lack of reviews for 31,980 of these 36,493 reports can be attributed to 816 IDRS managers who had not met the 90 percent certification rate requirement, which equates to almost 33 percent of all IDRS managers.

The IRS did not complete all corrective actions recommended in our prior review. Specifically, the IRS did not implement effective compliance reviews to ensure IDRS business divisions[3] were complying with IDRS security report requirements. The IDRS Security Program staff did not fully implement this recommendation because they had no means for enforcing IDRS business divisions to comply with IDRS security report requirements.

We also recommended in our prior review that IDRS managers be held accountable for their security report responsibilities. The IRS did not implement this recommendation because the

[3] IDRS business divisions are segments of IRS business organizations aligned to facilitate monitoring of taxpayer account accesses.

Cybersecurity organization believed action was no longer needed when the national average of certification rates improved.

Recommendations

We recommended that the Associate Chief Information Officer, Cybersecurity, 1) implement compliance review procedures for IDRS security officers that are designed to monitor and enforce IDRS business division compliance with security report responsibilities, 2) clarify what level of IRS organizational management should be assigned the responsibility for providing a response identifying corrective actions that are required for certification rates lower than 90 percent, 3) biannually provide a list of IDRS managers who have not met their IDRS security report responsibilities to the IRS business organization executive responsible for monitoring and enforcing IDRS business division and manager compliance with IDRS security program policy, and 4) complete plans to implement an enhancement in the IORS system to capture responses for IDRS business divisions when corrective actions are required for noncompliance.

The Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement should ensure IRS business organizations identify the executives responsible for monitoring and enforcing IDRS business division compliance with IDRS security program policy and providing a response identifying corrective actions for certification rates lower than 90 percent.

Response

IRS management agreed with the recommendations. The Associate Chief Information Officer, Cybersecurity, will 1) develop and implement compliance review procedures for IDRS security officers, 2) clarify the responsible level among IRS organizational management for submitting responses when certification rates are lower than 90 percent, 3) provide, at least biannually, IRS business organization executives responsible for monitoring and enforcing IDRS security compliance with a list of IDRS managers who have not met their IDRS security report responsibilities, and 4) implement an enhancement in the IORS system to capture responses for IDRS business divisions when corrective actions are required for noncompliance. In addition, the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement will issue a jointly signed memorandum reiterating IDRS security program policy requirements and will identify executives responsible for lower compliance rates. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

Table of Contents

Abbreviations

IDRS	Integrated Data Retrieval System
IORS	IDRS Online Reports Services
IRS	Internal Revenue Service

Background

The Taxpayer Browsing Protection Act of 1997[1] made it a criminal offense to access or inspect tax information without proper authorization. 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 primary 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.

It is a Federal crime for IRS employees to willfully access and view taxpayer accounts for other than tax administration purposes.

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 requires yearly training to be given to all employees to protect against it. Despite the training and existing security policies, UNAX violations continue to be an issue at the IRS. An internal IRS study reported that 1,191 UNAX cases had been processed by the IRS and the Treasury Inspector General for Tax Administration from Fiscal Year 2004 to Fiscal Year 2007.

Prior to November 2003, IDRS security staffs and managers of IDRS users 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 management reviews, the IRS deployed the IDRS Online Reports Services (IORS) system, which is a web-based application that makes IDRS security reports available electronically to authorized reviewers.

The IORS system notifies managers of IDRS users by email when IDRS security reports are available and when responses to reports are due. Managers of IDRS users are required to review and certify the following security reports on a regular basis to determine that IDRS users are accessing the IDRS for valid work requirements:

- Sensitive Access Report – Issued weekly, this report identifies IRS employees who have accessed another employee's or an employee's spouse's tax account.

[1] 26 U.S.C.A. Sections 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.

- Security Violations Report – Issued weekly, this report identifies attempted user transactions that violated specific IDRS security rules.
- IDRS Security Profile Report – Issued monthly and quarterly, this report identifies employees' IDRS capabilities.

The IRS Cybersecurity organization is responsible for overseeing compliance with the IORS system and has direct responsibility over IDRS Security Program staffs located in the IRS campuses.[3] IRS business organizations[4] are responsible for ensuring their IDRS managers comply with IORS system procedures, investigate potential security violations, and take appropriate corrective actions.

In a July 2006 audit report[5] on the IRS' use of the IORS system, we reported that a majority of IDRS managers were not reviewing or certifying IDRS security reports produced by the IORS system. The IRS Cybersecurity organization and IRS business organizations had not sufficiently emphasized the need for their IDRS managers to review the IDRS security reports produced by the IORS system. In addition, IDRS 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. Further, systemic problems with the IORS system contributed to the low compliance levels. We recommended that the Associate Chief Information Officer, Cybersecurity:

- Coordinate with the IRS business organizations and place emphasis on the review of electronic IDRS security reports using the IORS system.
- Conduct periodic compliance reviews to ensure IDRS business units[6] carry out their roles and responsibilities to review IDRS security reports.
- Hire a new contractor to complete development of the next version of the IORS system. The systemic weaknesses with the system should be prioritized and addressed within a reasonable time period.

[3] 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.
[4] IRS business organizations include the Criminal Investigation, Large and Mid-Size Business, Small Business/Self-Employed, Tax Exempt and Government Entities, and Wage and Investment Divisions; the Offices of Appeals and Chief Counsel; the Taxpayer Advocate Service; and the Agency-Wide Shared Services and Communications and Liaison functions.
[5] *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 24, 2006).
[6] IDRS business units are segments of IRS business organizations aligned to facilitate monitoring of taxpayer account accesses.

We also recommended that the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement:

- Ensure managers' operational review requirements are updated to include a step to validate that all IORS system-related reports are certified in a timely manner and to hold the managers accountable for meeting their security-related responsibilities.

This review was performed at the Cybersecurity organization office in New Carrollton, Maryland, during the period October 2008 through February 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Security Report Certification and Timeliness Rates Have Significantly Improved

About 50,000 IRS employees access the IDRS to process taxpayer data during the course of their normal work duties. For monitoring accesses to taxpayer accounts, IRS business organizations are segmented into field or campus units called IDRS business divisions. IDRS users are organized into IDRS units within the IDRS business divisions. Currently, the IRS has established 65 IDRS business divisions that oversee a total of 5,667 IDRS units.[7] IRS business organizations are required to appoint managers responsible for timely reviewing and certifying IDRS security reports for employees in their IDRS units, and identify a point of contact for coordinating overall IDRS security activities for each IDRS business division. For the purpose of monitoring the review and certification of IDRS security reports, the IRS further grouped IDRS business divisions by the 10 IRS campuses. IDRS security officers from the Cybersecurity organization are located at each of the 10 campuses to oversee and monitor the IDRS business divisions affiliated with their campus.

The IRS requires that managers of IDRS units maintain at least a 90 percent certification rate for their IDRS security reports. In addition, managers must certify weekly IDRS security reports within 14 calendar days and monthly IDRS security reports within 28 calendar days for the certifications to be considered as timely.

During this review, we found that the national averages of certification and timeliness rates for IDRS security reports have significantly improved since our last review. Figure 1 presents a comparison of the average certification and timeliness rates for the 10 campuses for Fiscal Year 2005 that were compiled by the Cybersecurity organization IDRS Security Program staff during our prior review, and the average rates for the 10 campuses for Fiscal Year 2008 compiled by the Cybersecurity organization IDRS Security Program staff during this review.

[7] Although not part of the IRS, the Treasury Inspector General for Tax Administration is included as 1 of the 65 IDRS business units because its employees may require access to the IDRS as part of their job responsibilities.

Figure 1: IRS Campus Security Report Certification and Timeliness Rates

	Certification Rate		Timeliness Rate	
IRS Campus	**Fiscal Year 2005**	**Fiscal Year 2008**	**Fiscal Year 2005**	**Fiscal Year 2008**
1. Andover	80%	90%	61%	78%
2. Atlanta	41%	73%	26%	60%
3. Austin	16%	74%	9%	63%
4. Brookhaven	88%	98%	68%	92%
5. Cincinnati	40%	85%	23%	69%
6. Fresno	42%	94%	26%	82%
7. Kansas City	59%	91%	35%	80%
8. Memphis	33%	94%	19%	83%
9. Ogden	78%	97%	55%	87%
10. Philadelphia	38%	87%	26%	72%
Averages	**54%**	**89%**	**37%**	**77%**

Source: Cybersecurity organization IDRS Security Program staff. Data were extracted using queries of the IORS system.

We attribute the improvements in the certification and timeliness rates to corrections and enhancements made by the IRS to the IORS system. In response to our prior review recommendations, the IDRS Security Program staff corrected IORS system problems that had hindered IDRS managers' ability to access IDRS security reports and were contributing to low certification and timeliness rates. In addition, the IDRS Security Program staff implemented system enhancements that further improved IDRS managers' compliance with completing their security report requirements, including:

- Automatic email messages to remind IDRS managers that certifications are due.
- A "report certification due" box on IORS system report screens that displays any reports that have not been certified and highlights past due reports in red.
- Actions and Certifications Detailed Reports that list which IDRS managers have and have not completed certifications. Campus security officers use this information to send weekly notifications to IDRS business unit points of contact for distribution to the appropriate IDRS managers who need to complete certifications.

Not All IDRS Business Divisions Are Complying With Requirements for Reviewing Security Reports to Protect Against Unauthorized Employee Accesses to Taxpayer Accounts

While the national averages of certification and timeliness rates for IDRS security reports has significantly improved, with the certification compliance rate getting close to the 90 percent, more needs to be done to ensure that all taxpayer accounts are protected from unauthorized access. The rates for some of the individual IDRS business divisions did not meet the certification and timeliness requirements. Of the total 325,475 security reports requiring certification by IDRS managers in Fiscal Year 2008, 36,493 (11 percent) were not reviewed and certified, potentially allowing improper accesses to taxpayer accounts to go undetected. Further analysis of the 36,493 reports identified that 32 of the 65 IDRS business divisions had certification rates that were lower than 90 percent for Fiscal Year 2008. The lack of reviews for 31,980 of these 36,493 reports can be attributed to 816 IDRS managers who had not met the 90 percent certification rate requirement, which equates to 32.7 percent of all IDRS managers. Fifty-seven of the 65 IDRS business divisions had at least 1 IDRS manager who did not meet the 90 percent certification rate requirement. Appendix IV presents the certification and timeliness rates for all 65 IDRS business divisions for Fiscal Year 2008.

In Fiscal Year 2008, 36,493 security reports were not reviewed and certified, potentially allowing improper access to taxpayer accounts to go undetected.

Effective compliance reviews were not implemented

IRS policy requires executives of business organizations with IDRS business divisions that do not have at least a 90 percent certification rate for their IDRS security reports to provide to the IDRS Security Program staff within 14 calendar days a response that identifies the nature and date of the actions to be taken to correct any deficiencies associated with the review and certification of security reports.

Based on the low certification and timeliness rates found during our prior review, we recommended that the IRS conduct periodic compliance reviews to ensure IDRS business divisions carried out their IDRS security report responsibilities. During this review, we found that the IRS had not yet implemented effective compliance reviews for monitoring IDRS business division compliance with IDRS policy.

The IDRS Security Program staff had taken some steps to implement this recommendation. In April 2006, they began to generate a quarterly report that listed the certification and timeliness rates for each of the 10 campuses. The staff shared this report with the IDRS Security Issues Committee that included representatives from the various IRS business organizations. However, in mid-2007, the IDRS Security Program staff discontinued providing this quarterly report to the

campuses because it was not getting distributed further. The quarterly report was not effective for informing IDRS business divisions of their certification and timeliness rates because the rates for individual IDRS business divisions were rolled up to the campus level. In addition, the IDRS Security Issues Committee members were serving as liaisons for their business organizations and not as monitors at the IDRS business division level.

In November 2006, the Memphis, Tennessee, Campus IDRS Security Program staff created draft compliance review procedures, *IORS Certification Standard Operating Procedures*, for IDRS security officers. These procedures instructed campus IDRS security officers to monitor report certifications in the IORS system on a weekly basis and notify IDRS business divisions at their campuses when report certifications become untimely. To perform this task, campus security officers used the Actions and Certifications - Detailed Utility Report feature in the IORS system to determine which IDRS managers had completed certifications and which had not. The security officers then emailed the reports to the IDRS business divisions' points of contact, who in turn distributed them to the appropriate IDRS managers who needed to complete certifications. Although these procedures were never finalized or formally issued, we found that IDRS security officers were generally following them and emailed weekly reports to inform IDRS managers when certifications were overdue.

However, the draft procedures did not instruct the IDRS security officers on what actions to take when IDRS managers did not complete their responsibilities. Also, the draft procedures did not instruct IDRS security officers to monitor IDRS business division certification and timeliness rates to determine those that had a lower than a 90 percent certification rate that required a response identifying the corrective actions they would take to improve compliance. For the 32 IDRS business divisions with certification rates lower than 90 percent, we found that none had provided a response identifying corrective actions.

The IDRS Security Program staff had not completed actions to implement compliance review procedures and was not enforcing the requirement for responses for IDRS business divisions with a lower than 90 percent certification rate for the following reasons:

- IRS business organizations had not identified executives to be responsible for providing the response for certification rates lower than 90 percent.
- IRS policy did not clarify what level of business organizational management should be assigned the responsibility for providing the response when needed.
- No mechanism existed to capture responses for noncompliant IDRS business divisions. The IDRS Security staff advised us that they intend to implement a mechanism to capture responses in the IORS system in December 2009.
- The IRS had not implemented any disciplinary mechanisms to help the IDRS Security Program staff enforce IDRS business division compliance with IDRS security reports requirements.

When IDRS managers do not complete certification of security reports in a timely manner, the IRS has no assurance that taxpayer accounts are being properly protected and potential unauthorized accesses to taxpayer data by employees are being identified.

Manager accountability was not implemented

Our prior review found that IDRS managers were not being held accountable for their IDRS security report responsibilities. We recommended that the IRS update the operational review requirements for its managers to include a step to timely certify all IORS security reports and to hold managers accountable for meeting their security-related responsibilities.

The National Institute of Standards and Technology Special Publication 800-100[8] describes the information security governance practices that are critical for ensuring the security of enterprise information assets. One of these critical practices is that individuals who are responsible for information security within the agency should be held accountable for their actions or lack of actions.

To address our recommendation, in Fiscal Year 2007, the IRS updated the self-assessment[9] that managers complete annually to include a step for IDRS managers to certify that they have completed their IDRS security report reviews. While the self-assessment may increase awareness of their IDRS security report responsibilities, it does not hold IDRS managers accountable if they do not comply with them.

The IRS had also planned to issue a memorandum signed jointly by the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement to IRS Commissioners and Chiefs requiring that all IRS business organizations identify and enforce disciplinary consequences for noncompliance with reviewing and certifying IDRS security reports. However, in June 2007, the IRS recorded an overall certification rate of 87 percent with a timeliness rate of 73 percent (up from a certification rate of 54 percent with a timeliness rate of 37 percent in Fiscal Year 2005). Based on the improvement in the national averages of certification and timeliness rates, the IRS Cybersecurity organization determined that no further action was needed to address manager accountability. As a result, the aforementioned joint memorandum was not issued. Consequently, the IRS did not identify or implement disciplinary consequences for IDRS managers who do not complete review and certification of IDRS security reports in a timely manner.

While certification and timeliness rates have improved, the rate of improvement has slowed. As discussed previously, 816 (32.7 percent) of IDRS managers did not meet the 90 percent certification rate requirement for security reports in Fiscal Year 2008. This contributed to 32 of

[8] *Information Security Handbook: A Guide for Managers*, published October 2006.
[9] IRS managers annually complete the Self-Assessment Tool for Managers to provide operational review information pursuant to the Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. Sections 1105, 1113, 3512 (2000).

65 IDRS business divisions having certification rates lower than 90 percent in Fiscal Year 2008; however, none of the divisions had provided a response identifying corrective actions. IRS business organizations had not identified executives to be responsible for monitoring and enforcing compliance with IDRS security policy and for providing the response identifying corrective actions for certification rates lower than 90 percent.

Because the IORS system tracks certification and timeliness data, the IDRS Security Program staff can generate a list of IDRS managers who have not met security report review requirements and provide this information to IRS business organizations to assist their monitoring and remediation of noncompliant IDRS managers. Strengthening IDRS managers' accountability for timely certification of IORS system security reports will increase the number of IDRS managers reviewing and certifying IDRS security reports, which will provide assurance that employees are accessing IDRS tax data for official purposes.

Recommendations

The Associate Chief Information Officer, Cybersecurity, should:

Recommendation 1: Implement compliance review procedures for IDRS security officers that are designed to monitor and enforce IDRS business division compliance with security report responsibilities and ensure that responses are obtained when corrective actions are required for noncompliance.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization has assembled a team to develop compliance review procedures for IDRS security officers and will work with the IDRS business divisions to finalize and implement these procedures.

Recommendation 2: Clarify what level of IRS business organizational management should be assigned the responsibility for providing a response identifying corrective actions that are required for certification rates lower than 90 percent.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization will work with the IDRS business divisions to clarify the responsible level among IRS business organizational management and will update IRS policy accordingly.

Recommendation 3: Biannually provide a list of IDRS managers who have not met their IDRS security report responsibilities to the IRS business organization executive responsible for monitoring and enforcing IDRS business division and manager compliance with IDRS security program policy.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization will, at least biannually, provide IRS business organization

executives responsible for monitoring and enforcing IDRS security program compliance with a list of IDRS managers who have not met their IDRS security report responsibilities.

Recommendation 4: Complete plans to implement an enhancement in the IORS system to capture responses for IDRS business divisions when corrective actions are required for noncompliance.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization will implement an enhancement in the IORS system to capture required responses from IDRS business division management and will update IRS policy to require the use of this IORS enhancement.

The Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement should:

Recommendation 5: Ensure IRS business organizations identify the executives responsible for monitoring and enforcing IDRS business division compliance with IDRS security program policy and providing a response identifying corrective actions for certification rates lower than 90 percent.

> ***Management's Response:*** The IRS agreed with this recommendation. A meeting will be held with IRS executive leadership to disseminate information on IRS noncompliance with IDRS security program policy. Executives responsible for providing a response when certification rates are lower than 90 percent will be identified. In addition, a jointly signed memorandum from the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement will be issued to division commissioners and functional chiefs reiterating the requirement to review and certify IDRS security reports maintained in the IORS system.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this review were to evaluate compliance by IRS management and security staffs in reviewing and certifying IDRS[1] security reports, which are produced online by the IORS system, and assess whether corrective actions taken to address our prior audit findings[2] were effective.

To accomplish our objectives, we:

I. Determined whether IRS business organizations are reviewing and certifying IDRS security reports using the IORS system in compliance with Internal Revenue Manual Section 10.8.34.

   A. Determined how the Cybersecurity organization compiles and validates the accuracy of the certification and timeliness rate information.

   B. Obtained the most current quarterly certification rate information, including the timeliness of the certifications, maintained by the IORS system and distributed quarterly by the Cybersecurity organization to IRS business organizations.

   C. Determined whether the Cybersecurity organization obtained written responses from executives of business organizations with lower than a 90 percent certification rate in accordance with IRS policy.

   D. Determined whether other monitoring or reporting corrective actions had been taken and whether they were effective.

II. Determined whether IRS business organization managers' operational review requirements were updated to include a requirement for timely certification of IORS system-related reports as well as consequences for noncompliance, in order to hold managers accountable for meeting their security-related responsibilities.

III. Determined whether the IORS system had been modified to address previously reported systemic problems, including system access issues, software problems, and management oversight issues.

[1] IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.

[2] *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 24, 2006).

A. Reviewed system change documentation to determine the corrections implemented and interviewed the IORS Project Manager to determine whether any ongoing problems were contributing to noncompliance in reviewing and certifying IORS system security reports.

B. Determined whether systemic corrective actions were effective in increasing compliance with reviewing and certifying IORS system security reports by interviewing IORS system users to solicit their opinions regarding the effectiveness of systemic changes made since the time of our last audit.

Appendix II

Major Contributors to This Report

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

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Chief Information Officer OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Director, Cybersecurity Programs and Policies OS:CTO:C:PP
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:
- Chief Technology Officer OS:CTO
- Chief Information Officer OS:CTO
- Associate Chief Information Officer, Cybersecurity OS:CTO:C

Appendix IV

IDRS Business Division Security Report Certification and Timeliness Rates for Fiscal Year 2008

3(d)

	IDRS Business Division	Total Reports	Certification Rate	Timeliness Rate
1	[redacted]	12	0.00%	0.00%
2		456	42.11%	31.58%
3		361	49.86%	44.88%
4		7,122	63.70%	50.82%
5		6,013	66.42%	57.51%
6		2,795	67.33%	51.06%
7		4,306	67.56%	47.91%
8		323	68.11%	48.92%
9		9,978	70.53%	56.30%
10		11,533	74.41%	42.73%
11		5,933	74.46%	63.16%

[1] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

3(d)

	IDRS Business Division	Total Reports	Certification Rate	Timeliness Rate
12	[redacted]	7,686	74.82%	53.93%
13		1,778	75.08%	64.74%
14		517	75.82%	67.70%
15		10,162	76.04%	68.02%
16		2,652	78.05%	64.14%
17		10,040	78.39%	64.76%
18		6,645	79.71%	67.71%
19		4,970	81.63%	64.14%
20		406	82.02%	71.72%
21		3,167	82.70%	71.87%
22		12	83.33%	83.33%
23		3,213	84.72%	78.49%
24		1,822	85.24%	68.44%
25		6,696	87.11%	63.35%
26		32	87.50%	53.13%

3(d)

	IDRS Business Division	Total Reports	Certification Rate	Timeliness Rate
27	[redacted]	8,952	87.63%	74.22%
28		342	88.01%	71.05%
29		11,419	88.41%	73.87%
30		3,176	88.85%	82.75%
31		1,883	89.54%	84.12%
32		4,496	89.72%	82.89%
33		72	90.28%	84.72%
34		7,460	91.26%	80.32%
35		360	91.39%	65.00%
36		9,768	91.55%	80.88%
37		6,089	91.72%	85.90%
38		3,888	92.34%	85.19%
39		2,208	92.62%	82.97%
40		12,076	93.42%	82.06%
41		2,893	93.61%	91.09%
42		1,831	93.72%	91.32%
43		663	93.97%	82.50%

3(d)

	IDRS Business Division	Total Reports	Certification Rate	Timeliness Rate
44	[redacted]	2,395	94.28%	76.95%
45		2,846	94.34%	87.43%
46		8,415	94.58%	81.82%
47		7,243	95.32%	89.69%
48		418	95.69%	87.80%
49		489	95.71%	86.09%
50		3,759	96.38%	89.78%
51		13,609	96.70%	86.00%
52		2,430	97.65%	72.10%
53		4,422	98.12%	94.41%
54		3,568	98.35%	88.31%
55		9,321	98.37%	95.39%
56		3,003	98.60%	96.17%
57		12,188	99.38%	90.36%
58		557	99.46%	91.02%
59		11,776	99.60%	94.74%

3(d)

	IDRS Business Division	Total Reports	Certification Rate	Timeliness Rate
60	[redacted]	11,976	99.66%	89.91%
61		11,204	99.87%	84.09%
62		15,340	99.89%	89.31%
63		13,028	99.97%	97.36%
64		1,014	100.00%	96.55%
65		268	100.00%	89.55%
	Total/Averages	**325,475**	**89%**	**77%**

Source: Cybersecurity organization IDRS Security Program staff. Data were extracted using queries of the IORS system.

Appendix V

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

RECEIVED
AUG 13 2009

August 13, 2009

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report – Progress Has Been Made, but Additional Steps Are Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses
(Audit #200820020) (i-trak #2009-61928)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate the report recognizing that the Internal Revenue Service:

- Improved significantly in its national average regarding certification rates for manager reviews of Integrated Data Retrieval System (IDRS) security reports for their employees, specifically, from 54 percent in fiscal year 2005 to 89 percent in fiscal year 2008.
- Improved significantly in its national average rate of timely manager reviews of IDRS security reports, specifically, from 37 percent in fiscal year 2005 to 77 percent in fiscal year 2008.
- Enhanced the IDRS Online Reports Services System that provides electronic security reports to managers for review.

The Service's Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes; your suggested recommendations will further improve our security posture. We agree with and will implement all of your recommendations as specified in the attachment.

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Agnes Spruill at (202) 283-7018.

Attachment

Attachment

Draft Audit Report – Progress Has Been Made, but Additional Steps Are Needed To Ensure Taxpayer Accounts Are Monitored To Detect Unauthorized Employee Accesses (Audit #200820020) (i-trak 2009-61928)

RECOMMENDATION #1: The Associate Chief Information Officer, Cybersecurity, should implement compliance review procedures for IDRS security officers that are designed to monitor and enforce IDRS business division compliance with security report responsibilities and ensure that responses are obtained when corrective actions are required for noncompliance.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. Cybersecurity has assembled a team to develop compliance review procedures for IDRS security officers. Cybersecurity will work with the Business Units to finalize and implement these procedures, which will be included in IRS policy IRM 10.8.34.

IMPLEMENTATION DATE: February 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Associate Chief Information Officer, Cybersecurity, should clarify what level of IRS business organizational management should be assigned the responsibility for providing a response identifying corrective actions that are required for certification rates lower than 90 percent.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will work with Business Unit points of contact to clarify the responsible level among IRS business organizational management. IRS policy IRM 10.8.34.8.3(4) will be updated to clarify the responsible level of management for submitting responses.

IMPLEMENTATION DATE: February 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Associate Chief Information Officer, Cybersecurity, should biannually provide a list of IDRS managers who have not met their IDRS security report responsibilities to the IRS business organization executive responsible for monitoring and enforcing IDRS business division and manager compliance with IDRS security program policy.

Attachment

Draft Audit Report – Progress Has Been Made, but Additional Steps Are Needed To Ensure Taxpayer Accounts Are Monitored To Detect Unauthorized Employee Accesses (Audit #200820020) (i-trak 2009-61928)

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. Cybersecurity will, at least biannually, provide IRS business organization executives responsible for monitoring and enforcing IDRS security compliance with a list of IDRS managers who have not met their IDRS security report responsibilities.

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Associate Chief Information Officer, Cybersecurity, should complete plans to implement an enhancement in the Integrated Data Retrieval System Online Report Services (IORS) to capture responses for IDRS business divisions when corrective actions are required for noncompliance.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Cybersecurity will implement an enhancement to IORS to capture required responses from business division management. IRM 10.8.34 will be updated to require the use of this IORS enhancement.

IMPLEMENTATION DATE: April 1, 2010

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #5: The Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement should ensure IRS business organizations identify the executives responsible for monitoring and enforcing IDRS business division compliance with IDRS security program policy and providing a response identifying corrective actions for certification rates lower than 90 percent.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. A meeting will be held with executive leadership to disseminate information on IRS noncompliance with IDRS security program policy. Executives responsible for providing a response when certification rates are lower than 90 percent will be identified. In addition a jointly-signed memo from the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and

Attachment

Draft Audit Report – Progress Has Been Made, but Additional Steps Are Needed To Ensure Taxpayer Accounts Are Monitored To Detect Unauthorized Employee Accesses (Audit #200820020) (i-trak 2009-61928)

Enforcement will be issued to Division Commissioners and Functional Chiefs reiterating the requirement to review and certify JDRS security compliance reports maintained in IORS.

IMPLEMENTATION DATE: December 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.