Security Over Taxpayer Data Used in Conducting Compliance Research Should Be Improved

September 2000

Reference Number: 2000-20-159

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 25, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Over Taxpayer Data Used in Conducting Compliance Research Should Be Improved

This report presents the results of our review of security controls over taxpayer data in the Internal Revenue Service's (IRS) Office of Research. In summary, we found that the Office of Research did not always obtain the proper approvals in requesting taxpayer data, restrict access to taxpayer data, and ensure controls to detect unauthorized accesses were followed. We recommended that additional controls be established to ensure proper approvals are obtained and that security deficiencies be corrected.

IRS management generally agreed with our findings and recommendations. Their written response discusses several corrective actions that will improve the reported conditions. Management's comments have been incorporated into the report where appropriate, including some minor changes to terminology used in the draft report. The full text of their comments is included as an appendix.

While we concur with all corrective actions, we do not agree that four of the seven corrective actions have been completed, as reported in management's response. The modernization of the Office of Research and the ongoing centralization of the IRS' information systems resources under the Chief Information Officer affect the implementation of these corrective actions.

Copies of this report are also being sent to IRS managers who are affected by the report recommendations. Please call me at (202) 622-6510 if you have any questions, or your staff may contact Scott Wilson, Associate Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

Table of Contents

Executive Summary

The Internal Revenue Service's (IRS) Office of Research conducts analyses to identify tax noncompliance issues, root causes for the issues, and practical approaches to modify non-compliant behavior. To perform their jobs, Office of Research employees have access to millions of taxpayer records. Assuring the security of these records is important to avoid unauthorized disclosure, misuse or loss of taxpayer data. The objective of this review was to determine if the Office of Research adequately safeguarded taxpayer data used in research efforts.

Results

We identified three security issues in the Office of Research where taxpayer data was not adequately secured against the risks of unauthorized disclosure, misuse, and loss. During our review, we became aware of potential inappropriate accesses to computer workstations at one Office of Research site that could have led to the theft or improper disclosure of taxpayer data. These access attempts are being investigated by the Treasury Inspector General for Tax Administration's Office of Investigations.

Office of Research Employees Obtained Taxpayer Data Without Receiving Proper Approvals

Approvals ensure that research plans have adequately presented detailed project information, including data needs and security. Over half of the projects we reviewed did not have proper approvals from the responsible executive as required, yet employees working those projects obtained taxpayer data.

Office of Research Management Did Not Always Properly Restrict Access to Taxpayer Data

Access controls provide assurance that those without authorization are not allowed access to sensitive data. Office of Research sites had security weaknesses that hindered their ability to limit access to taxpayer data on a need-to-know basis.

Office of Research Management Did Not Always Follow Controls to Detect Unauthorized Accesses

The main detection control available on computer systems is the audit trail, which provides a track record of key accesses to taxpayer files. Office of Research sites were not consistently activating and reviewing audit trails, and, in some cases, did not maintain adequate separation of duties for adding, deleting or modifying data on the research systems.

Summary of Recommendations

To reduce the risk of unauthorized disclosure, misuse, and loss of taxpayer data, we recommend that all requests for taxpayer data be approved, as required. We also recommend that access to taxpayer data used in research be limited and monitored.

Management's Response: IRS management generally agreed with our findings and recommendations. The modernization of the Office of Research and the centralization of the Information Systems Division affected the implementation of some of the corrective actions. In light of the modernized Research offices, the policies and procedures that address our findings will be carried over into the Operating Divisions, which will take over jurisdiction of the various District Office Research and Analysis sites throughout the country. In addition, a newly created council will provide oversight and coordination over the implementation of corrective actions.

Management's complete response to the draft report is included in Appendix IV.

Office of Audit Comment: While we concur with all of the corrective actions, we do not agree that four of the seven corrective actions have been completed, as reported in management's response. The corrective actions cited generally describe actions and events that will occur in the future versus actions that have already been implemented.

Objective and Scope

The objective of this review was to determine whether the Office of Research adequately safeguarded taxpayer data used in research efforts.

The objective of our review was to determine whether the Internal Revenue Service's (IRS) Office of Research adequately safeguarded taxpayer data used in research efforts. Taxpayer data consisted of Taxpayer Identification Numbers (TIN), taxpayer names, taxpayer addresses, and tax practitioner TINs.

We conducted our review from October 1999 to May 2000 in the Office of Research headquarters in Washington, D.C., and District Office Research and Analysis (DORA) sites in Atlanta, Fort Lauderdale, Los Angeles, and St. Louis. This audit was performed in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

At the time of our review, the IRS' Office of Research employed over 370 employees located in its headquarters office and 33 supporting DORA sites. Its mission is to contribute to improving voluntary compliance by conducting data-driven research to identify tax noncompliance issues, root causes for those issues, and practical actions to modify non-compliant taxpayer behavior. To perform their jobs, Office of Research employees have access to millions of taxpayer records.

In 1998, the IRS began taking actions to modernize the way it does business so it can provide taxpayers top quality service. This required fundamental changes in almost all aspects of the IRS, including its research activities. One of the first changes made was to the name of the organization from Compliance Research to the Office of Research. This better reflected the expansion of focus from taxpayers' compliance

treatments to other forms of solutions (e.g., electronic tax administration and customer service). While all plans have yet to be finalized for the Office of Research, preliminary plans have the DORA sites being embedded into the four Operating Divisions[1] and one National Headquarters site. The specific roles and responsibilities have yet to be determined. Because the IRS has not finalized the role of the Office of Research, our audit results were based on its current structure.

Results

The Office of Research did not maintain adequate security over taxpayer data.

Actions need to be taken to improve the security of taxpayer data used by the Office of Research. Employees obtained taxpayer data without proper approvals, access to the data was not always properly restricted, and controls to detect unauthorized accesses were not always followed.

By tightening the security controls surrounding the use of taxpayer data, the IRS will be able to provide more assurance to the public that taxpayer data used in research efforts are properly approved and sufficiently secured to minimize the risk of unauthorized disclosure, misuse, and loss.

Office of Research Employees Obtained Taxpayer Data Without Receiving Proper Approvals

To ensure taxpayer data are not misused, all projects must be approved by a responsible executive.

The Office of Research requires approvals of research plans to ensure they address the objective, methodology, data needs, anticipated benefits, budgetary constraints, milestones, and privacy and security issues for each research project. Currently, projects that are national in scope require the approval of the Director, Office of Research, or Assistant Commissioner (Research and

[1] Wage and Investment, Small Business and Self-Employed, Large and Mid-size Business, and Tax-Exempt/Government Entities.

Statistics of Income), and projects that are local in scope require the District Director's approval. The Director, Office of Research, issued a memorandum in March 1999 to DORA Chiefs on the approval process to reinforce the established procedures.

Approximately one-half of the projects we reviewed did not have the approval from the responsible executives.

The 30 projects we selected used taxpayer data from 14.8 million taxpayers and consisted of 22 national and 8 local projects. For purposes of this test, we excluded 7 of the 22 national projects. One of the 7 was still in the development stage, and 6 of the projects were related and did not need separate approvals. Eight of the remaining 15 national projects had not been approved by the Director, Office of Research, or the Assistant Commissioner (Research and Statistics of Income), and 4 of the 8 local projects had not been approved by the District Director.

Even without the proper approvals for the 12 projects above, DORA employees obtained over 5.9 million taxpayer records from other divisions in their local offices and in the National Office to proceed with their work.

When employees obtain taxpayer data without approvals, the IRS becomes vulnerable to disclosure violations and misuse of the data.

There are inherent risks in using taxpayer data, such as unauthorized disclosure, misuse, or loss of that data. By not following established guidelines, the vulnerability to these risks increases.

These conditions occurred because managers and employees did not give sufficient weight to obtaining proper authorization for using taxpayer data. Also, the Office of Research had no central control to ensure approvals were received. Local projects were not controlled on the national inventory of projects, which prevented headquarters management from being aware of what projects were ongoing and what kinds of data were being used.

Recommendations

1. The Assistant Commissioner (Research and Statistics of Income) should assign accountability to an official as the approving authority over all

research projects. In light of the IRS modernization, the appropriate Director over the research function in each Operating Division should implement this recommendation.

Management's Response: The guidance policy currently in place will likely be carried over into the modernized Research program. Within each Operating Division, field Research managers will report directly to senior Research management, ensuring these policies are observed. The modernized Research program includes both a Senior Management Council and a Research Data and Technology Council to oversee and coordinate these efforts.

Office of Audit Comment: While we agree with management's corrective action on this recommendation, we do not agree that this corrective action has been completed, as cited in their response. Completion of this corrective action will occur when policies and procedures have been established for the four Operating Divisions' Research functions and when a single point of authority has been assigned accountability over the approval process.

2. The Assistant Commissioner (Research and Statistics of Income) should ensure that DORA employees do not receive data with taxpayer identifiers from other IRS functions without the appropriate approval. Managers and employees obtaining data without appropriate approvals should be referred to the Treasury Inspector General for Tax Administration's (TIGTA) Strategic Enforcement Division for investigation of potential violations of the statutory rules governing unauthorized access and inspection of taxpayer records by IRS employees (referred to as UNAX).

Management's Response: Giving the Chief Information Officer (CIO) and the Information Systems (IS) Organization sole control over information technology resources will substantially remove the likelihood of "back-door" data acquisition. The Research Data and

Technology Council will develop specific procedures for ensuring compliance with data acquisition policies.

Office of Audit Comment: While we agree with management's corrective action on this recommendation, we do not agree that this corrective action has been completed, as cited in their response. Completion of this corrective action will occur when specific procedures for ensuring compliance with data acquisition policies have been developed and implemented in each Operating Division.

3. The Director, Office of Research, should ensure all local projects are added to the national inventory of projects. By adding local projects to the national inventory, headquarters management would be aware of what projects were ongoing and what kinds of data were being used. Another benefit would be to reduce the potential duplication of effort among projects. In light of the IRS modernization, the appropriate Director over the research function in each Operating Division should implement this recommendation.

Management's Response: The modernized Research design will substantially reduce the volume of local projects, thus ensuring that all projects will be national in scope and included in each Operating Division's national inventory of projects.

Office of Research Management Did Not Always Properly Restrict Access to Taxpayer Data

Access controls provide assurance that those without authorization are not allowed access to sensitive data. Guidance on IRS system security comes from the Internal Revenue Manual[2] (IRM) section on Data Processing Services and the IRS' Office of Security, Evaluation and Oversight.

[2] The IRM contains operating procedures for all IRS functions.

Office of Research sites had security weaknesses involving access to taxpayer data, which hindered their ability to restrict access to data on a need-to-know basis.

To highlight the importance of security controls, 1 DORA site discovered approximately 21 failed access attempts to several of its workstations during our review.

Access to taxpayer data on Office of Research computer systems was not sufficiently limited to those who needed it. The importance of access controls was illustrated when, during our review, 1 DORA site identified approximately 21 failed attempts to access several computers. The attempts were made from other IRS offices and were suspicious enough that DORA referred the incidents to TIGTA's Office of Investigations for further investigation. This indicates that unauthorized access attempts do occur and proper security settings can be critical in protecting taxpayer data. The conditions cited below increase the risk of unauthorized disclosure, misuse, and loss of taxpayer data.

- The Office of Research allowed employees in its headquarters office to use non-standard operating systems on workstations connected to its network. Operating systems provide key controls to authenticate and identify users. The IRS' standard operating system is Microsoft Windows NT. The non-standard operating systems included operating systems for Apple (Apple OS) and Sun Microsystems (Solaris) computers. There were at least 10 Apple computers in operation. Neither operating system had been evaluated for conformity to the level of security required for systems that process taxpayer information. The Department of the Treasury and the IRM requires that connectivity to any IRS system must be certified and authorized in writing to ensure that the connecting system will not degrade the security present on the host system.
- The Office of Research headquarters allowed some users to load applications on its workstations. For example, some employees had loaded their preferred versions of Microsoft's Internet Explorer. The IRM requires only authorized personnel to load approved software on IRS systems. The risks of computer virus outbreaks and security breaches increase significantly when users are allowed to load their own software.

- One DORA site maintained a laptop computer that contained two operating systems, Windows NT and Windows 95. Because a user can access either operating system, the security benefits from Windows NT can be bypassed. Windows 95 cannot effectively prevent any user from accessing information stored on the computer.

Security concerns include the use of unauthorized operating systems and software packages, weak access and password settings, existence of unauthorized user accounts, and the lack of physical security over back-up tapes.

- DORA employees in one site were given permissions to view and delete files of projects that they were not assigned to work. In addition, DORA network servers at two sites were not properly configured to require a certain password length and the frequency on how often a password must be changed. This would prevent unlimited attempts to access the system by unauthorized users. The Department of the Treasury and the IRS require that access to sensitive data be given only to authenticated users on a need-to-know basis.
- Two separated employees still had access to the Office of Research network and data because their user accounts were not disabled or deleted from the network after they left the Office of Research. However, neither had used the passwords to access the network after leaving. One of the two separated employees also had physical access to Office of Research workspace, including the computer room. This employee's building access card, which was coded for access to Office of Research floors and the computer room, was not deactivated upon separation. We could not determine whether the employee accessed the computer room because access records were maintained for only a limited time.
- Back-up tape storage of Office of Research data did not properly limit access. The back-up tapes from two key databases and the headquarters office file servers were stored in a small, moveable combination safe in an unrestricted area at the IRS headquarters office. This area could be entered at seven doors, one of which was unlocked and used by several employees from other divisions.

The conditions cited above occurred because the Office of Research sites did not comply with IRS security procedures and other local guidelines. There were also inconsistencies from site to site on whether IS or DORA employees were responsible for administering DORA's computer systems.

Recommendations

4. Office of Research management should ensure all security deficiencies are corrected. Specifically, they should:

    - Ensure standardized operating systems and applications are installed and running on all Office of Research computer resources.
    - Restrict user rights and permissions to match employee assignments and apply standard password configurations to Office of Research resource servers.
    - Verify that separated employees have had their user accounts disabled or deleted, and that their building access privileges have been taken away.
    - Improve physical security over their back-up tapes to ensure the tapes and the information on the tapes are secured and only accessible by authorized personnel.

Management's Response: The Office of Research sites addressed many of these issues as they were identified during the audit. Furthermore, giving the CIO/IS Organization sole control over information technology resources will substantially address all of these issues. This will permit a uniform set of information technology standards to be applied to all Research systems.

5. Responsibility for managing the Office of Research's computer systems should be transferred to the CIO. This would ensure more compliance with IRS security standards. IS currently has responsibility for administering virtually every other computer system in the IRS. Systems administrators

reporting to the CIO should be held accountable for ensuring access control standards are followed.

Management's Response: The IRS expects that giving the CIO/IS Organization sole control over information technology resources will substantially address all of these issues. System administrator responsibilities previously in the Office of Research will be transferred to the IS Organization on October 1, 2000.

Office of Research Management Did Not Always Follow Controls to Detect Unauthorized Accesses

Controls to detect improper accesses to computer systems consist of the activation of the audit trail function and review of audit trail information. Audit trails are historical records of key access control occurrences, such as who made the access, what they did, and when it occurred. Audit trails should be reviewed and analyzed regularly by an employee who does not have the capability to add, delete, or modify data on the system. The two places within the Office of Research where audit trails should be activated and reviewed are at the resource server and the workstation.

We identified two issues in regards to the audit trail function within the Office of Research.

Detection weaknesses involved not using audit trails to identify inappropriate computer accesses and the inadequate segregation of duties for reviewing audit trails.

- Audit trails were not consistently activated and reviewed from site to site. Audit trail reviews were conducted for both servers and workstations in two of five sites. One site had both audit trails activated, but only conducted reviews on the server. Another site activated and reviewed the audit trails at the workstation level, but did not activate the audit trail function at the server level. The remaining site had the function activated, but did no reviews.
- Employees who conducted audit trail reviews also had the ability to access, disable, and/or alter the audit trail logs in two sites that conducted audit trail reviews. These individuals were provided

administrator privileges to perform other duties within the office.

These detection issues existed because Office of Research sites did not comply with IRS security procedures and other local guidelines. The importance of correcting the above conditions can be demonstrated through incident reports turned in by Office of Research sites where audit trail reviews were conducted. Out of the five sites we visited, three sites filed six incident reports, two for each site, that involved computer access attempts in the last three years. All incidents involved attempts to access DORA workstations by users who were not known by the DORA reviewers.

The incidents are summarized as follows:

- Repeated successful logons by an "Anonymous User" from another IRS office. The user had administrator rights, which allows for the addition, modification, and deletion of records. Based on the available information, we could not determine the specific actions the user had taken.
- Twenty-one failed access attempts on eight different workstations, as mentioned earlier. The attempts were made by three different non-DORA users from other IRS offices. These attempts were referred to TIGTA's Office of Investigations for further review. These attempted accesses were adequately resolved.
- Twenty-three failed login attempts by an administrator on two different computers.
- Ten failed access attempts by non-DORA users.
- Ten failed access attempts by an administrator to the Compliance Data Warehouse (CDW).[3]
- Unspecified number of failed access attempts to the CDW by an employee.

[3] The CDW is one of two main research database systems available to all Office of Research employees.

Because the Office of Research did not consistently review audit trails and because duties were not adequately separated, management could not state with confidence who had tried to access their system, what they did, and when.

Recommendations

6. Office of Research management should ensure the audit trail function is activated at the server and workstation levels at each site.

Management's Response: The IRS expects that giving the CIO/IS Organization sole control over information technology resources will substantially address this finding. The Office of Research will apply appropriate uniform standards on activating audit trail features on all Research systems.

Office of Audit Comment: While we agree with management's corrective action on this recommendation, we do not agree that this corrective action has been completed, as cited in their response. Completion of this corrective action will occur when the CIO establishes the uniform standard on enabling the audit trail functions and Research offices activate the audit trail features on all Research systems.

7. Office of Research management should assign the audit trail review duties to someone who does not have system administrator duties. In light of the IRS modernization, the appropriate Director over the research function in each Operating Division should implement this recommendation.

Management's Response: The Research Data and Technology Council will develop specific actions to address audit trail reviews by Research managers.

Office of Audit Comment: While we agree with management's corrective action on this recommendation, we do not agree that this corrective action has been completed, as cited in their response. Completion of this corrective action will occur when

specific actions to address audit trail reviews have been developed and implemented in each Operating Division.

Conclusion

The Office of Research needs to improve security over taxpayer data. The use of millions of taxpayers' records for research efforts inherently creates the risk for possible disclosure and misuse issues. When controls to minimize these risks are not followed, the IRS is unnecessarily exposed to these risks.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of our review was to determine whether the Internal Revenue Service's (IRS) Office of Research adequately safeguarded taxpayer data used in research efforts.

I. We determined if the Office of Research sites were using live taxpayer data (i.e., data containing taxpayer identifiers, such as Taxpayer Identification Numbers, names or addresses) in accordance with laws, regulations and policies.

A. We identified congressional concerns and IRS policies and current practices regarding the use of live taxpayer data and the conditions for using such data, with emphasis on taxpayer disclosure and privacy. We also identified public records related to the Office of Research function and any available public comments to Privacy Act notices, and compared the information to its current policies, procedures, and controls.

B. We determined whether the Office of Research headquarters office maintained a management information system for monitoring and controlling projects using live taxpayer data.

C. We determined if Office of Research sites maintained operational controls over projects to ensure the projects and the use of project data were properly authorized.

1. We requested District Office Research and Analysis (DORA) management's assistance to identify 190 open projects where taxpayer identifiers were included as part of the projects' data files. We stratified the projects by location to identify and select the sites with the highest number of projects, with the exception of the headquarters site. We visited five sites and reviewed 54 projects: Atlanta, Georgia (17 projects), Ft. Lauderdale, Florida (9 projects), Los Angeles, California (13 projects), St. Louis, Missouri (12 projects) and the Office of Research in Washington, D.C. (3 projects). We eliminated 24 of the 54 projects that were not conducted during Fiscal Years 1998 and 1999, did not actually contain taxpayer identifiers, or had taxpayer identifiers removed prior to use.

2. We interviewed Office of Research team members and reviewed the project plans, project prospectuses, and data certifications for the remaining 30 projects in our review. Because the 30 projects included 6 duplicate projects from 3 national strategies and 1

project in its developmental stages, we reviewed the 23 applicable projects for each item below:

- Whether taxpayer identifiers requested were essential for their analyses and were consistent with the project's objective.
- Whether the request contained the proper approvals prior to the data being requested and received for analysis.
- Whether the data requested are permitted under privacy and disclosure guidelines.
- Whether the sites retained taxpayer data on their networks or individual workstations.
- The number of taxpayers and taxpayer accounts used for projects.

II. We determined if Office of Research sites were adequately configuring their automated information systems to maximize logical security for restricting access to taxpayer information. We conducted our reviews in the headquarters office in Washington, D.C., and DORA sites in Atlanta, Fort Lauderdale, Los Angeles, and St. Louis.

A. We evaluated access controls over computer systems and data containing taxpayer identifiers to ensure personnel were authorized access to such systems and data on a need-to-know basis.

B. We identified three current/active and all former employees (departing in 1998 or 1999) who had Office of Research automated information system access and determined if they still had a valid reason for the access.

C. We selected three available employees in each office and determined if their individual workstation security settings met standards and policies.

D. We determined if automated information systems, user passwords, rights, permissions, and privileges were configured to meet IRS and/or industry standard security settings on Windows NT.

E. We determined if automated information system operating system security configurations met IRS and/or industry security standards, including appropriate system access restrictions, file and application installation restrictions and directory/file level access restriction controls.

F. We assessed the administration and configuration of telecommunications security including, use of encryption, use of modems, and the use of remote access systems capabilities, and physical protection of data lines.

G. We assessed the use of automated information system audit trails.

1. We determined if audit trails were being effectively reviewed, and that any suspicious incidents were properly reported.

2. We determined if adequate separation of duties existed between administrators and audit trail reviewers.

III. We determined if the Office of Research sites maintained adequate security over their automated information system facilities to protect access to taxpayer information. We conducted our tests in the same offices as in step II above.

A. We interviewed local security managers, DORA and security services personnel, and conducted on-sight inspections of Office of Research facilities where taxpayer data are stored, including computer rooms and off-premises back-up tape storage areas, to assess the security level.

B. We reviewed Office of Research self-assessments on physical security to identify any control weaknesses.

C. We interviewed functional security coordinators and identified and reviewed one incident report which involved missing or stolen computer equipment within DORA sites to ensure that controls had been implemented to effectively identify and respond to security-related incidents.

D. We interviewed Information Systems support personnel, and observed data back-up procedures and storage facilities to identify control weaknesses.

1. We evaluated the controls implemented to ensure data file back-up procedures effectively protected against the loss of data.

2. We verified available documentation and inventory listings of back-up tapes stored off premises for accuracy and reliability.

3. We interviewed pertinent management and office personnel to determine the cause for and recovery of any omitted tapes.

E. We identified Office of Research personnel who had separated or transferred and who still had access to Office of Research space.

Appendix II

Major Contributors to This Report

Scott Wilson, Associate Inspector General for Audit (Information System Programs)
Stephen Mullins, Director
Kent Sagara, Audit Manager
Louis Lee, Senior Auditor
Bill Lessa, Senior Auditor
Abe Millado, Senior Auditor
Billy Benge, Auditor
Christina Johnson, Auditor
Midori Ohno, Auditor
Beverly Tamanaha, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Information Officer IS
Chief Operations Officer OP
Assistant Commissioner (Research and Statistics of Income) OP:RS
Deputy Chief Information Officer (Operations) IS
Director, Office of Research OP:RS:R
Office of Security and Privacy Oversight IS:SPO
Director, Office of Program Evaluation and Risk Analysis M:O
The Office of the Chief Counsel CC
The Office of Management Controls CFO:A:M
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Audit Liaisons:
- Assistant Commissioner (Research and Statistics of Income) OP:RS
- Information Systems Audit Assessment and Control IS

Appendix IV

Management's Response to the Draft Report

COMMISSIONER

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

September 15, 2000

RECEIVED
SEP 15 2000
4:25PM

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Response to Draft Audit Report – Security over Taxpayer Data Used in Conducting Compliance Research Should Be Improved (Audit No. 19990081)

Thank you for the opportunity to respond to your draft report entitled "Security over Taxpayer Data Used in Conducting Compliance Research Should Be Improved." The report is a review of our research program, at the National level and in four districts, including on-site inspections made during the first quarter of Fiscal Year (FY) 2000 and a review of a sample of national and local projects from FYs 1998 and 1999.

Let me begin by clarifying the differences in the mission and roles of our Research organization as depicted in the draft report and that of Research in the modernized IRS. The draft report focuses on the "Compliance Research program." However, early in 1998 we changed the name of our organization to the Office of Research to reflect the expansion of our focus from taxpayers' compliance behavior to other forms of non-compliance related behavior, for example, electronic tax administration, customer service, filing burdens. This broadened focus will continue to characterize the mission of the five Research organizations in the modernized IRS.

Even in its original vision, our Research program's principal mission was not an adjunct to enforcement or targeting taxpayers for audit. Rather, we set up the program to use research results to develop alternatives to traditional enforcement. Yet, in your cover letter and at several points in the draft report, there is a repeated focus on a perceived "risk of targeting taxpayers for compliance actions" – almost an implication that any secondary uses of taxpayer data in our research environment are somehow improper or illegitimate. This implication is not supported by my reading of the facts gathered during the audit itself. In fact, the System of Records notice published in the Federal Register in December 1998 that covers research systems (cf. 63 Federal Register 69890) does not recognize the restrictions that are implied at several points in your cover letter and draft report. We have legitimate research uses of taxpayer data that may directly or indirectly lead to enforcement contacts. For example, the Research organization develops scientific formulas for selecting enforcement workload. Such formulas can

only be developed and tested using taxpayer data. Likewise, when noncompliant taxpayers fail to respond to a non-enforcement activity, we need to be ready to apply traditional enforcement actions. Research can use taxpayer data to define noncompliant groups more tightly and, in so doing, limit the scope of enforcement actions. Hence, we do not concur with your assessment that minimizing the risk of targeting taxpayers for compliance actions is an applicable benefit of your recommendations.

Clearly, whenever taxpayer data is used for research of any sort, I am concerned that we use all appropriate security measures. I do agree that we have not consistently done all we could to ensure that taxpayer information used for research was adequately secured against unauthorized disclosure, misuse, and destruction. I believe the various actions underway as part of our modernization effort will help us make progress in addressing these concerns. One of the five drivers of change that I identified early as needed to guide modernization was management roles with clear accountability. The principal deficiencies your report identified were due not to lack of clear policy guidance, but to divided responsibilities and management's failure to ensure such guidance was consistently followed. As we move forward with modernization, I believe giving the Chief Information Officer organization ownership of all IRS information technology resources (including data) and having field Research managers report directly to senior managers in each Operating Division's Research organization will improve the deficiencies you identified.

We have yet to settle many of the details of how our Research program will operate within the four Operating Divisions and Headquarters. The new Research executives will have to address a number of transition issues. High on the list of such issues will be how to transition existing policy guidance including dealing with securing taxpayer data. The recommendations in this report will also become a transition issue. I have given the new Headquarters Research organization the lead role in coordinating security and data acquisition issues to ensure common practice across the Research organizations. Additionally, the Technology Security Council, which was established in August 1999 and is currently being reconstituted to reflect our modernization, will review all policy guidance concerning security. The mission of this Council, chaired by the Chief Information Officer, is to discuss technology security requirements Servicewide.

Our responses to the specific recommendations in this report are as follow:

RECOMMENDATION #1
The Assistant Commissioner (Research and Statistics of Income) should assign accountability to an official as the approving authority over all research projects. In light of the IRS modernization, the appropriate Director over the Research function in each Operating Division should implement this recommendation.

ASSESSMENT OF CAUSE(S)
In a sample of projects using taxpayer data, the Treasury Inspector General for Tax Administration (TIGTA) found eight national projects and four local projects which did not have a project plan signed by either the Assistant Commissioner (Research and Statistics of Income) for national projects or the District Director for local projects. TIGTA believes this represents a failure to establish a central control to ensure approvals were received.

CORRECTIVE ACTIONS
The report acknowledges the basic adequacy of the underlying policy guidance that is already in place and that is likely to carry over into the modernized Research program. The issue of clarifying management roles and responsibilities and ensuring we observe and enforce these policies lies within each Operating Division's Research organization and, as appropriate, across all such organizations. Field Research managers will report directly to senior Operating Division Research management ensuring these policies are observed. The Headquarters Research design includes both a Senior Management Council and a Research Data and Technology Council to oversee and coordinate these efforts.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Directors, Customer Research, Operating Divisions
Director, Headquarters Research and Analysis

CORRECTIVE ACTION(S) MONITORING PLAN
Not applicable.

RECOMMENDATION #2
The Assistant Commissioner (Research and Statistics of Income) should ensure that DORA employees do not receive data with taxpayer identifiers from other IRS functions without the appropriate approval. Managers and employees obtaining data without appropriate approvals should be referred to TIGTA's Strategic Enforcement Division for investigation of potential violations of the statutory rules governing unauthorized access and inspection of taxpayer records by IRS employees, referred to as UNAX.

ASSESSMENT OF CAUSE(S)
Based on its review of a sample of research projects, TIGTA believes that managers and employees have not given sufficient weight to obtaining proper authorization for using taxpayer data.

CORRECTIVE ACTIONS
The standard policy governing data acquisition for research projects is that data can only be acquired with approval of a project plan by the Assistant Commissioner (Research and Statistics of Income), for national projects, or by the District Director, for local projects. In the instances cited by the report, managers and employees used taxpayer data properly and acquired it in good faith based upon approval of national operational initiatives (which included a research component) by an official superior to the Assistant Commissioner (Research and Statistics of Income) – the Chief Operations Officer. The IRS expects that giving the Chief Information Officer/Information Systems (IS) organization sole control over information technology resources will substantially remove the likelihood of "back-door" data acquisition. The Research Data and Technology Council, whose membership will include a representative of the Chief Information Officer/IS organization, will develop specific monitoring procedures for ensuring compliance with data acquisition policies.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Directors, Customer Research, Operating Divisions
Director, Headquarters Research and Analysis

CORRECTIVE ACTION(S) MONITORING PLAN
Not applicable.

RECOMMENDATION #3
The Director, Office of Research, should ensure all local projects are added to the national inventory of projects. By adding local projects to the national inventory, another benefit would be to reduce potential duplication of efforts among projects. In light of the IRS modernization, the appropriate Director over the Research function in each Operating Division should implement this recommendation.

ASSESSMENT OF CAUSE(S)
Based on its review of eight local research projects, TIGTA found that in four instances data was being used without the written approval of the District Director. TIGTA believes the lack of a national inventory of projects prevented Headquarters management from knowing about ongoing projects and the data used in them.

CORRECTIVE ACTIONS
I participated actively in the design of the modernized IRS Research program. One of my beliefs is that the major issues and challenges of tax administration are national in scope, not local, and can best be addressed by research that is national in focus. That belief had a practical effect on the ultimate design of the four Research organizations

within the Operating Division – namely, that field research sites would not report to management in their geographic locale, as they have in the past, but rather to Headquarters management. I believe that implementation of this design will substantially reduce the volume of research efforts focusing on a narrow geographic area and will ensure that any such research would be approved and controlled by Headquarters Research management in each of the Operating Divisions.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Directors, Customer Research, Operating Divisions

CORRECTIVE ACTION(S) MONITORING PLAN
Not applicable.

RECOMMENDATIONS #4 and #5
Compliance Research management should ensure all security deficiencies are corrected. Specifically, they should:

- Ensure standardized operating systems and applications are installed and running on all Compliance Research computer resources.
- Restrict user rights and permissions to match employee assignments and apply standard password configurations to Compliance Research resource servers.
- Verify that separated employees have had their user accounts disabled or deleted and that their building access privileges have been taken away.
- Improve physical security over their back-up tapes to ensure the tapes are secured and only accessible by authorized personnel.

Responsibility for managing Compliance Research's computer systems should be transferred to the Chief Information Officer.

ASSESSMENT OF CAUSE(S)
TIGTA found that 10 Apple computers and other computers were operating in the Headquarters office with non-standard operating systems whose security had not been certified. Some users could load applications onto their own workstations. One laptop in the field had both Windows 95 and NT loaded. Inappropriate access permissions were found at one site. Network servers at two sites did not conform to password standards. Two separated employees retained network and data permissions after their separation and one of these retained physical access to the workspace. Back-up storage tapes were stored in a non-secure IS-controlled location.

CORRECTIVE ACTIONS
The Research organization has used its interactions with the TIGTA auditors to address many of these issues as they were discovered during the audit. Furthermore, the IRS expects that giving the Chief Information Officer/IS organization sole control over information technology resources will substantially address these issues. System administrator responsibility previously in the Research organization will be transferred to the Chief Information Officer/IS organization on October 1, 2000. This will permit a uniform set of information technology standards to be applied to all Research systems. Specifically,

- All Research workstations are now part of INOMS and we will evaluate the security of non-standard hardware and operating systems and replace it, if necessary, as part of our hardware and Windows 2000 replacement efforts.
- All applications on Research systems are now subject to Servicewide standards and to the process for seeking waivers on other than non-standard software.
- Forms 5081 are being used consistently to grant access to Research systems.
- System and physical access permissions have been revoked for the separated employees identified by TIGTA; such permissions are now normally revoked the day an employee separates from service.
- New procedures will require systems administrators to certify that access permissions have been revoked as part of the normal process for employee separations.
- A new password scheme was implemented approximately eight months ago that exceeds current IRS standards. This new scheme also includes all NT password security features.
- User accounts inactive for 30 days are locked and access is denied.
- The Information Systems organization has taken corrective actions to secure the area used for back-up tape storage.

We also expect that, as the modernized Research function begins its operations, the Research Data and Technology Council may suggest other actions to address this recommendation.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Director, Office of Research
Chief Information Officer

CORRECTIVE ACTION(S) MONITORING PLAN
Ensure that the Research Data and Technology Council, once operational, continues to address computer security issues.

RECOMMENDATION #6
Compliance Research management should ensure the audit trail function is activated at the server and workstation level at each site.

ASSESSMENT OF CAUSE(S)
In a review of five sites that identified several instances of successful log-ins by an anonymous user from another IRS office and many more instances of failed log-in attempts, TIGTA found that management does not consistently review audit trails.

CORRECTIVE ACTION
The IRS expects that giving the Chief Information Officer/IS organization sole control over information technology resources will substantially address the issues identified by TIGTA. We will apply appropriate uniform standards immediately on activation of audit trail features on all Research systems. If additional actions become necessary, we expect the Research Data and Technology Council will address them.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Director, Office of Research
Chief Information Officer

CORRECTIVE ACTION(S) MONITORING PLAN
Ensure that the Research Data and Technology Council, once operational, continues to address computer security issues.

RECOMMENDATION #7
Compliance Research management should assign the audit trail review duties to someone who does not have system administrator duties. In light of the IRS modernization, the appropriate Director over the Research functions in each Operating Division should implement this recommendation.

ASSESSMENT OF CAUSE(S)
In a review of five sites that identified several instances of successful log-ins by an anonymous user from another IRS office and many more instances of failed log-in attempts, TIGTA found that employees who conduct audit trail reviews also had the ability to access, disable, and/or alter audit trail logs.

8

CORRECTIVE ACTIONS
The IRS expects that giving the Chief Information Officer/IS organization sole control over information technology resources will substantially address the issues identified by TIGTA. System administrator duties will be transferred to IS employees. We also expect the Research Data and Technology Council will develop specific actions to address audit trail reviews by Research managers.

IMPLEMENTATION DATE
Completed.

RESPONSIBLE OFFICIALS
Director, Office of Research
Chief Information Officer

CORRECTIVE ACTION(S) MONITORING PLAN
Ensure the Research Data and Technology Council, once operational, continues to address computer security issues.

If you have any questions, or need additional information, please contact me, or a member of your staff may contact Ellie Convery, Acting Assistant Commissioner (Research and Statistics of Income), at (202) 874-0100.